



Hogan  
Lovells

# GMCQ

Global Media Technology and  
Communications Quarterly

Spring 18

# Editorial

Virtually every industry is being reshaped with the use of Artificial Intelligence (AI) and advanced machine-learning, ranging from healthtech to self-driving vehicles, to education and smart homes, drones and space, social media, and everything in between and beyond. These new technologies present a variety of commercial opportunities and the potential to change our daily lives. At the same time, new AI innovations bring many legal, policy, commercial and strategic challenges that need to be considered across jurisdictions. In this issue we analyse the legal and regulatory issues businesses should be thinking about now when it comes to AI.

Who should take responsibility when AI causes harm? Richard Diffenthal and Helen McGowan of our London Tech Hub team talk to Karen Yeung, Interdisciplinary Professorial Fellow of Law, Ethics and Informatics at the University of Birmingham and one of our Academics Advisory Panel members, about the case for regulating AI.

Is AI the ultimate test for privacy? Eduardo Ustaran, head of our London privacy team, explores the tension between our need for data in order to successfully develop AI and the data privacy and cybersecurity legal frameworks which are being developed around the world and which impact that use of data.

Who owns the IP in the output of an AI? Penny Thornton and Imogen Ireland in our London IPMT team look at questions of IP ownership and infringement in light of current UK intellectual property laws.

Winston Maxwell and Sam Choi take a close look at the data privacy laws impacting any 'big data' project, including AI projects where data is being analysed and provide tips on how to stay compliant with the GDPR, which comes into force next month.

Next we hear from IBM France's General Counsel, Bruno Massot, who is also part of a global working group on Blockchain, on what IBM is doing in the area of blockchain and the challenges his in-house team face.

Turning our attention to the United States and the ongoing discussion around 'net neutrality', our Washington D.C. communications team take a look at the FTC's role in monitoring broadband markets going forward and bringing actions against ISP's for anti-competitive behaviour.

Trey Hanbury interviews our market leading Silicon Valley M&A partners Rick Climan, Keith Flaum, Jane Ross and John Brockland for their views on global trends in technology transactions and working in Silicon Valley.

Nils Rauer and Andreas Doser of our Frankfurt office outline the key aspects of the recent Commission proposal for a regulation on the free-flow of non-personal data across borders and look at the practical challenges of the regulation for businesses.

Finally, our China and Hong Kong partners explore the growing trend for foreign investors to partner with Chinese cloud license holders in order to enter the Chinese cloud services market.



**Winston Maxwell**  
Partner  
Paris



**Trey Hanbury**  
Partner  
Washington, D.C.



**Penelope Thornton**  
Senior Knowledge Lawyer  
London

# Contents

04	Artificial Intelligence – time to get regulating?
10	Is Artificial Intelligence the ultimate test for privacy?
12	Are the UK's intellectual property laws ready for AI?
16	The starting point for a big data project: the privacy impact assessment
30	A blockchain-proof legal department: insights from Bruno Massot – IBM France
35	A preview of the FTC's role in monitoring broadband markets following the FCC's adoption of the Restoring Internet Freedom Order
40	Tech M&A: the view from the Valley
46	The new European framework on the free flow of non-personal data
53	Evolving landscape for international cloud providers in China: why US technology giants are pairing up with local partners
61	References



# Artificial Intelligence – time to get regulating?



The buzz regarding the potential for artificial intelligence ("AI") to revolutionise our lives is inescapable. Development of AI technology is a huge growth area, and investors are banking on an "AI boom" in everything from cybersecurity and healthcare<sup>1</sup>. The capabilities and achievements of AI in some areas are certainly astonishing – self-driving cars are no longer theoretical but a reality, and AlphaGo is now arguably the strongest Go player in history<sup>2</sup>. But the picture isn't all rosy, which the Economist has recently described as a 'Techlash' against the digital giants. As with any technology, there are negative as well as positive effects of AI. Applications of AI in social media can help us find long-lost friends, but those same channels can be manipulated to disseminate fake news and influence our decisions. Are these and other similar worries matters of public concern that warrant a societal response? AI applications, whether it's a smart city, logistics management or build to order (BTO) and just-in-time manufacturing can be optimised to increase efficiency but who should take responsibility when automated processes cause harm?

In light of these emerging externalities, many, Elon Musk included, have called for structured regulation of AI to manage and control the risks. But is regulation the answer? We explored some of the current issues and debates with Karen Yeung, Interdisciplinary Professorial Fellow in Law, Ethics and Informatics at the University of Birmingham.

A common concern often voiced about regulation of new technologies is that if we intervene with regulation too early, we might impede the potential of the innovation by imposing controls, constraints and additional expense. This can deter investment and discourage development of the technology. On the other hand, if we delay in taking action because we are concerned about inhibiting development, then it may become too late to do anything about the risks and harms that have already been generated. Karen agrees this so-called 'tech control dilemma' (or Collingridge dilemma, as it is sometimes called) presents a real challenge for AI. She also warned, however, that pitting innovation and regulation against one another in those terms creates a false dichotomy. In her experience there are both beneficial innovations, which we should encourage, as well as unhelpful or potentially harmful innovations, the effects of which we should aim to mitigate.

“

A serious challenge is managing for bias in the underlying data on which most AI algorithms are built.

”

“

It is possible that through use of AI, our environment will become so smart and pre-emptive that all of our choices will be structured and manipulated in ways that will ultimately reduce our capacity to make authentic free independent choices.

”

Considerable public attention has been given to risks that AI might pose that are more existential in nature. For Karen, this is not primarily a concern about fears that we will create some kind of general AI taking over the world. Rather, *"it is possible that through use of AI, our environment will become so smart and pre-emptive that all of our choices will be structured and manipulated in ways that will ultimately reduce our capacity to make authentic free independent choices."* We are already seeing the impact of this through the echochamber of social media, dissemination of fake news and misinformation, all of which have the potential to shape our environment and influence our collective beliefs and actions.

On that basis, the case for regulation in theory sounds convincing. But will it be achievable in practice? AI is a universal technology that crosses borders and disciplines. Establishment and implementation of a regulatory framework for this complex area is no simple task, and in the view of some, almost impossible. Karen does not share this view, noting that China has done an extraordinarily effective job at regulating access to the internet from mainland China, providing an illustration of what can be done with focused efforts and resources, although she hastened to add that she was certainly not advocating state censorship along the lines adopted in China. Nonetheless, Karen remarked, *"I don't really buy the argument that it's completely unreasonable to regulate AI or that it's too big a task to take on. It's certainly challenging, and I think that technological mechanisms for ensuring that certain standards are implemented will be vital, given the scale on which these technologies operate, but I don't buy the argument that it's too difficult for us to get a handle on it. Where there's a will there's a way."*

A critical aspect of any regulatory framework for AI will be allocation of responsibility for AI based outcomes. In Karen's view, the assessment is relatively straightforward where the AI decisions are subject to meaningful human review – the human reviewer takes ultimate responsibility. It becomes more difficult when you fully automate the decision, like who gets a loan, or who gets a job interview, and so on, if these decisions are not subject to human review. In the classic example of a self-driving car which is programmed to take decisions based on an in-built risk assessment process, who takes responsibility for the outcome of those decisions? The data scientist that designed the relevant algorithms? The car owner? The manufacturer? The car occupants? Karen observes that these debates are challenging our intuitive and long understood social conventions about how we should attribute responsibility. She explained that the behaviour of AI systems that are capable of learning is emergent and therefore unpredictable, and that the AI might be harnessed by bad actors for malign purposes, or simply used in contexts for which it was never intended. Arguably therefore, software developers and others in the supply chain should not be responsible where they could not have reasonably foreseen a particular outcome. The difficulty with that position is that the resultant loss may then lie with the innocent victims, a position that Karen finds untenable. *"The solution," she said, "may be to think about allocation of risk in different ways than current social conventions dictates. For example, in the case of driverless cars, maybe the right answer is to have a mandatory insurance scheme that would bear the risk such that none of the software developer, nor the manufacturer, nor the victim, bears liability."*

Is regulation the right tool to achieve this? If allocation of liability is essentially the result of a social contract, is there a risk that in regulating the development and use of AI, we impose social norms which, on the plus side, might embody certain ideals, but which fail to keep pace with the changes in fast developing technologies and which only serve to reinforce biases? Karen points out that the claim that 'technology outpaces law' does not imply that we should therefore forgo attempts to mitigate against the serious and genuine risks that these technologies may generate. She also explained that *"regulation is meant to promote certain kinds of objectives and values, so to the extent that bias is just another word for embodying particular values then I think that's unavoidable. The important thing is that those objectives and values should be articulated and transparent, and subject to democratic deliberation."* In her view, a more serious challenge is managing for bias in the underlying data on which most AI algorithms are built. She said that we see historic forms of discrimination inherent in the underlying data and these biases



are then replicated due to the way the algorithms operate. Karen referred to one study that found that men were shown high paying job ads six times more often than they were shown to women because historically women have been statistically less likely to apply for high paying jobs than men. The algorithm that generated the ads was based on its analysis of historic data, which showed that women were not placed in high paying jobs and thus *inferred* from these historic patterns that women are thus less interested than men in high paying jobs. She explained that, *"this kind of bias is really problematic because our society has historically discriminated against certain vulnerable groups. I'm not sure whether you can in fact correct for that kind of historic bias that is embedded into our social structures. The data available to us includes these inherent biases and if we tried to correct it there wouldn't be any data upon which to train an algorithm."*

Part of the problem in regulating AI is that if we rely on AI to make decisions we do not always know how the AI system reached that decision, and so it becomes difficult to explain the process behind how certain decisions were reached. This is critical in the context of any regulatory framework, where, absent strict liability, the ability and opportunity to give reasons and justifications for taking certain actions is central to the allocation of liability. In Karen's view, the importance of explainability varies according to context. How and why an algorithm concluded that it should recommend the purchase of a book or similar item is probably of little consequence to most people, whereas in contexts such as the provision of legal advice, medical diagnosis, and parole releases, explainability becomes extremely important and the decision-makers need to be able to offer an explanation that they can defend. As Karen highlighted, in those highly consequential contexts *"it's unlikely to be acceptable just to say, 'well the machine said so!'"*. But in order to do this Karen suggested that we need to get much better at a formal mathematical verification systems and testing. Her view is that, alongside any regulatory framework, we need to develop robust methods for verifying the validity of the outcomes, and that these methods need to be available and accessible to professionals in all sectors, not just data scientists and coders.



In light of these issues concerning the influence of social conventions on the development of regulation, we asked Karen if we are leaning towards AI regulation on a piecemeal basis, with individual countries developing their own standards and approaches, having regard to individual countries', culture, customs, and existing legislative frameworks. Karen responded that in an ideal world we would have global cooperation on some core baseline principles, whilst allowing scope for divergence where that is culturally and politically legitimate and appropriate, but it seems unlikely that we will be able to coordinate a truly global approach. For example, as between the UK and the US, the US approach to regulation of risks such as data privacy and maintenance of individual freedom of choice, is much less robust than the European approach. On that basis she does not realistically see that there will be *"any serious regulatory collaboration across the Atlantic."*

Karen's views are consistent with others working in this space. Various themes are emerging with respect to the shape of AI regulation concerning transparency, accountability, obligations to manage for bias in the algorithm or underlying data and provision of mechanisms for testing and verifying AI based outcomes. Nesta has gone one step further by putting together a suggested set of standards for the use of AI by public sector organisations<sup>3</sup>. These include requiring that any use of AI is accompanied by a description of its function, objectives and intended impact, ensuring that where AI is deployed, a human being takes responsibility for the outcomes of AI decision making, and publishing risk assessments for mitigating potential biases.

So Elon Musk may be right that AI represents a public risk, and it may now be time to put serious thought into nature of the externalities generated by AI in order to develop a regulatory framework to manage those externalities. As Karen emphasised, even if those risks are unlikely to materialise in the form of James Cameron's *The Terminator*, *"AI has the potential to erode our autonomy and our freedom in ways that we might not even notice, if it is allowed to continue unchecked, unexamined and unregulated."*

“

AI has the potential to erode our autonomy and our freedom in ways that we might not even notice, if it is allowed to continue unchecked, unexamined and unregulated.

”

**Richard Diffenthal**

Partner, London  
T +44 (20) 7296 5868  
richard.diffenthal@hoganlovells.com

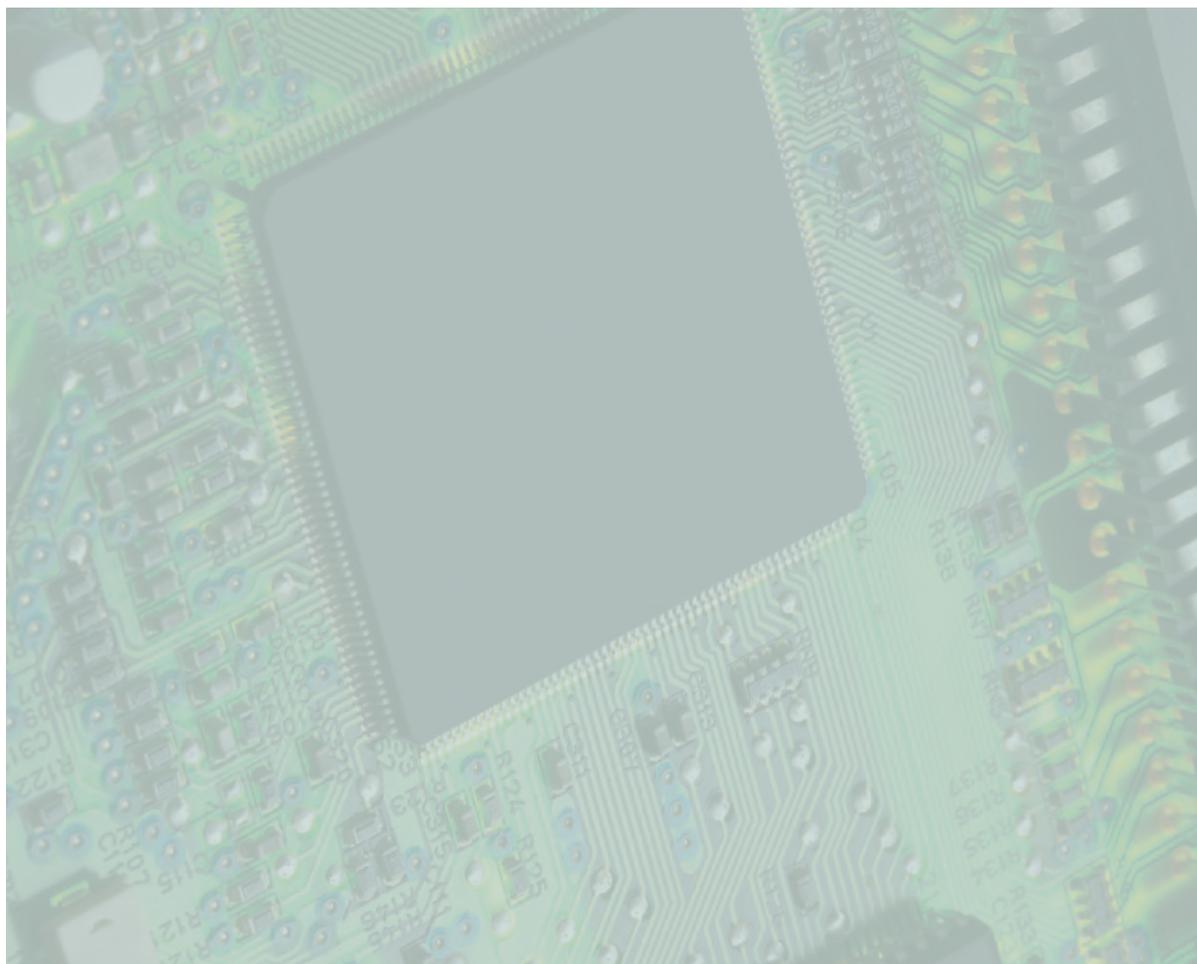
**Helen McGowan**

Associate, London  
T +44 (20) 7296 5581  
helen.mcgowan@hoganlovells.com

**Professor Karen Yeung**

Birmingham Law School  
Interdisciplinary Professorial Fellow in Law, Ethics and Informatics  
T +44 (0)121 414 6298  
pa-ipflawandethics@contacts.bham.ac.uk

Karen Yeung is the University of Birmingham's first Interdisciplinary Chair, taking up the post at the University of Birmingham in the School of Law and the School of Computer Science in January 2018. She has been a Distinguished Visiting Fellow at Melbourne Law School since 2016. She is a Fellow of the University's recently established Institute for Global Innovation (IGI), leading the 'Responsible Artificial Intelligence' challenge theme which supports over 50 researchers from a wide range of disciplines from across the University.



# Is Artificial Intelligence the ultimate test for privacy?



Nothing challenges the effectiveness of data protection law like technological innovation. You think you have cracked a technology neutral framework and then along comes the next evolutionary step in the chain to rock the boat. It happened with the cloud. It happened with social media, with mobile, with online behavioural targeting and with the Internet of Things. And from the combination of all of that, artificial intelligence is emerging as the new testing ground. 21st century artificial intelligence relies on machine learning, and machine learning relies on...? You guessed it: Data. Artificial intelligence is essentially about problem solving and for that we need data, as much data as possible. Against this background, data privacy and cybersecurity legal frameworks around the world are attempting to shape the use of that data in a way that achieves the best of all worlds: progress and protection for individuals. Is that realistically achievable?

At a practical level, sourcing the data required for machine learning to happen is the first battleground. The volume of data available is not a problem in itself given the exponential growth of our digital interactions. But in many cases, the ability to magically crunch the necessary data will rest with those that provide services to the owners of the data. Using European data protection jargon, those developing artificial intelligence are often processors rather than controllers. The limited decision-making power of processors when it comes to the use of data can be a serious handicap. To what extent can a vendor of technology services to a hospital use the patient data to develop more effective services? Should a cloud provider be entitled to access data it does not own to enhance its offering? The potential benefits of these activities can be substantial but they may not be directly enjoyed by the controller. However, with the right level of openness, cooperation and creativity it should be possible to enable those vendors to use their insights from the provision of the services and still retain their role as processors.

“

This is not a machine v. human battle. It is a defining moment which requires a sense of responsibility and a long-term view.

”

A knottier legal issue is the lawful ground for the processing of personal data in the context of the development of artificial intelligence. The uneasy relationship between consent, contractual necessity and legitimate interests comes firmly to the fore in this area. Obtaining consent for something that is so difficult to understand is never going to be straightforward. Justifying such data processing activities on the basis that they are necessary for the performance of a contract involving the data subject only gives a very narrow margin. So as with many other daily uses of personal information, we are left with the wobbly option of relying on legitimate interests, which is not in itself sufficient when dealing with special categories of data like data concerning health or biometric data – both of great relevance to applications of artificial intelligence. The key thing to remember here is that the legitimate interests ground places the onus on those wishing to exploit the data to show that no matter how clever and useful the outcome of that exploitation, it must not place an intolerable burden on people's right to privacy.

And whilst technology becomes increasingly complicated, so does the law. A worrisome legal complication arising in this respect is the uncertain interpretation of the European right not to be subject to a decision based solely on automated processing that significantly affects an individual. Although stated as a right, regulators are adamant that it should be seen as a requirement for explicit consent unless it can fit within the contractual necessity exemption or is authorised by EU or Member State law.

As a result, much of the ability to allow machines to make decisions affecting people will be linked to how relevant those decisions are to our lives. Shopping recommendations generated by algorithms? No big deal. Being eligible for a certain school, a career-defining promotion or life-saving medical treatment? Get a human involved pronto. Whether humans themselves will be able to make the right decisions without blindly relying on machines is perhaps one of the big questions of our time.

Ironically, assessing the impact of technology on our privacy and identifying the right safeguards may end up being more accurately done by machines in the not too distant future. Until then, our principal job will be to embed privacy and cybersecurity practices in the development of artificial intelligence involving personal data. New legal principles such as data protection by design and by default should guide this process whilst allowing for pragmatism and common sense. This is not a machine v. human battle. It is a defining moment which requires a sense of responsibility and a long-term view. Future generations will thank us if the way in which we develop artificial intelligence today looks at the true value it can deliver while respecting data protection principles.

*This article was first published in Data Protection Leader in February 2018.*



**Eduardo Ustaran**  
Partner, London  
T +44 20 7296 5249  
eduardo.ustaran@hoganlovells.com

# Are the UK's intellectual property laws ready for AI?

"AI doesn't just belong to a few tech giants in Silicon Valley"<sup>4</sup>: these were the words of Google Cloud's chief scientist for AI, Fei-Fei Li, speaking in March 2018 at a panel discussion on the impact of AI. Whilst companies such as IBM, Microsoft and Google have been at the forefront of AI for a number of years, many organizations across many different industries, are now looking to jump on the bandwagon, as AI continues to permeate the public consciousness. In response to the gathering momentum behind AI, thought-leaders in AI are calling for a careful look at how we should prepare. As Fei-Fei Li put it, we need to "*really study the profound impact of AI to our society, to our legal system, to our organizations, to our society to democracy, to education, to our ethics.*" In 2017 the UK Government commissioned a Select Committee to consider the economic, ethical, social and legal implications of AI. Against this backdrop, we ask whether or not the UK's intellectual property laws are ready for AI, and look at what businesses can do to prepare.

Before we can answer this question we need to consider what is meant by "AI". Popular culture has provided us with multiple examples of AI, such as "Samantha" from the 2013 film, *Her* and "Ava" from the 2015 film, *Ex Machina*. Both are intelligent computer operating systems capable of thought and consciousness. For many, this idea – computers that have the ability to reason, communicate and perform like a human – is the epitome of AI. Yet AI can also include computing advances that extend a human's ability to sense, learn and understand. An AI platform that is able to work through and analyse data in order to establish new data points or patterns, can

enhance a human activity. In the healthcare industry, for example, AI is being developed to analyse huge volumes of data to understand patient symptoms and provide suggested treatment options. In the automotive industry, autonomous vehicles are being developed to navigate roads and avoid other cars or pedestrians, to enable humans to move from A to B. Yet there is an important difference between the "Samantha" and "Ava" examples and the examples of AI platforms just given. The former is completely autonomous, whilst the latter requires collaboration with, or intervention by a human.

A purely autonomous form of AI could involve computers interacting with other computers and making decisions or carrying out functions without any human involvement. This form of AI where, crucially, there is no human agency at any stage, could pose problems for traditional legal structures such as intellectual property laws. For example, an AI that develops an invention without any human involvement would be the "inventor" of that invention. Yet under UK patent laws an inventor is defined as a person. Could this stretch to include an AI? Further, should this stretch to include an AI? Presently a person who discloses their novel and inventive invention to the state is given a 20 year monopoly. This is referred to as the "patent bargain". It rewards the hard work and dedication that is often invested in devising inventions. Yet, compared to humans, AIs have and will have an even greater ability to process considerably larger amounts of data at far quicker rates. Autonomous AIs could therefore arrive at their own inventions without any of the serendipity or hard work behind human invention. Is it appropriate for the state to reward such an AI with a 20 year monopoly for its invention? Would the answer be different if the AI develops a patentable invention with huge benefits for society?

But let's not get carried away. Undoubtedly AI is coming, but is it here yet? The common consensus is that it is not. Whilst enormous progress has been made in AI and machine

learning – examples of which we've discussed in relation to, the healthcare or automotive industries – we are still a way off creating fully autonomous AIs. The decision-making behind a human/AI collaboration is not fully autonomous, because it is limited by the parameters provided in the initial computer program design and algorithms. In this scenario, where the AI amounts to human written software code, arguably the software programmer could qualify as the "inventor" of any patentable outcome. But should that always be the case? Is it right that the software programmer should be able to patent that invention, even if the invention was an unintended and unforeseeable result of the AI? Should a person benefit from the patent monopoly if the invention was derived from analysing large amounts of public data? Developments in AI – whether looking at fully autonomous AIs or human/AI collaborations – prompt important questions about who should benefit from the patent monopoly.

Similarly, what happens if an AI output is a work protected by copyright? For example, a piece of music, or an art work, or even a new algorithm. Under UK copyright laws, the author of computer-generated literary, dramatic, musical or artistic works, is the person "by whom the arrangements necessary for the creation of the work are undertaken".<sup>5</sup> "Computer-generated" is defined "as a work generated in circumstances such that there is no human author of the work". Under UK copyright law therefore the





software programmer would most likely be the author and first owner of a copyright work generated by an AI. The position will be more complicated and unclear however in relation to more sophisticated AI which involves human collaboration and input at various stages of development of the AI. For example, teams of programmers and multiple companies, working on the design of algorithms and determining and providing the data sets to be analysed. In that scenario there may be multiple joint owners. Moreover, is it right that the output of an AI should be protected by copyright at all? Copyright only protects "original" literary, dramatic and artistic copyright works. Originality under UK copyright law means sufficient 'skill, labour and judgment' has been expended. Does the output of an AI involve the right kind of skill and labour to be afforded protection? Is it sufficient that skill and labour was involved in writing the algorithm that generated the AI? Another interesting question is whether the position would be different in other EU countries? Copyright protection for computer-generated works is not currently harmonised in Europe and the EU test for originality is whether or not the work is the "author's own intellectual creation", which requires a human author. The UK government may well choose to diverge from the rest of Europe on protection for AI-created works post-Brexit.

The example of an AI that infringes IP has been cited as another possible challenge to current IP laws, the argument being that we do not have the legal infrastructure to hold an AI accountable for infringement. Certainly there may be enforcement issues if the IP infringement is committed by a *fully autonomous* AI. However, the present sophistication of AI is such that there is likely to be a person – whether a designer, implementer, tester or user of the controlling software – behind it. It should still be possible to hold that "ultimate person(s)" accountable under current laws. Whilst it may be harder to trace the ultimate person(s), such a scenario does not challenge the fundamentals of IP infringement law, yet. Arguably the UK common law system is well set up to deal with technological developments, since case law can evolve to accommodate new factual scenarios. However, as developments in AI progress, the dividing line between AIs that have a human agent, and AIs that are fully autonomous, will blur. It may not be so easy to work out whether an AI's decision to infringe or create IP is ultimately attributable to a human.

Although the UK Government's Select Committee has been considering the legal implications of AI, the focus is on safety and regulation rather than intellectual property laws. Pending changes in the law to clarify the position on ownership of AI-created IP and given the likelihood that there may be some litigation in this area, organisations should check now and ensure that any new agreements relating to the development and use of AI clearly state which part(ies) should own any protectable IP resulting from the AI.

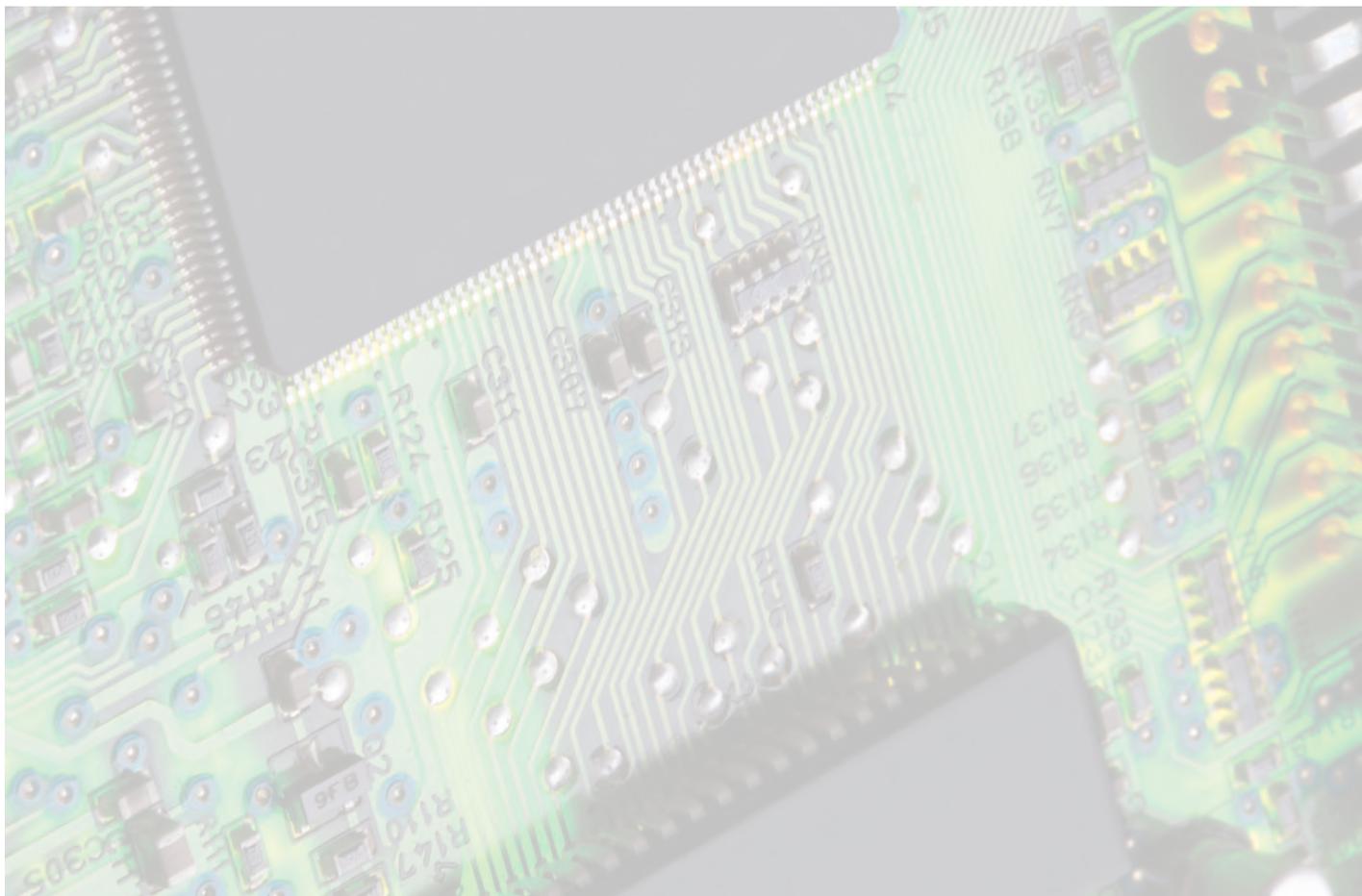
---



**Imogen Ireland**  
Associate, London  
T +44 20 7296 2158  
imogen.ireland@hoganlovells.com



**Penny Thornton**  
Senior Knowledge Lawyer, London  
T +44 20 7296 5665  
penelope.thornton@hoganlovells.com



# The starting point for a big data project: the privacy impact assessment



The era of big data is here. Not only do we generate more data than ever before, we now have the tools to analyse it to make inferences, predictions and even decisions. The use of big data analytics has spread throughout the public and private sectors, with applications in fields as diverse as health, education, financial services, retail, marketing and online services. And though we have yet to see the full potential of big data, it is already proving to be invaluable to businesses, helping to provide services more efficiently, streamlining recruitment and customer onboarding processes and improving the effectiveness of marketing campaigns. However, the use of big data has also been the source of much controversy, particularly where it involves sensitive information, concerns children, minorities or other vulnerable people, or where the decision-making has a significant impact on individuals. As both public interest and regulatory scrutiny in artificial intelligence, machine learning and big data continues to build, it is increasingly becoming important for businesses to be aware of individuals' rights over their data and be prepared to demonstrate compliance with data protection laws.

This is particularly the case for organisations working with data about individuals in Europe, as the regulatory framework on data protection is set to change with the EU General Data Protection Regulation (GDPR) coming into force on 25 May 2018. One of the innovations of the GDPR is the introduction of the focus on accountability, which is the requirement to not only comply with the obligations of the GDPR but also be able to demonstrate compliance with the GDPR. The data protection impact assessment (DPIA), also called privacy impact assessment (PIA), is an important tool that organisations have at their disposal to ensure that their processing of personal data complies with data protection law and minimises the impact on privacy. This guide is intended to explain why, when and how PIAs should be carried out in the context of a big data project. It also discusses some of the key issues that are likely to be identified in a PIA on a big data project and factors to consider when making risk-based decisions on the basis of a PIA.

“

One of the innovations of the GDPR is the introduction of the focus on accountability.

”



### Why carry out a privacy impact assessment

Big data projects, by virtue of their definition, involve data. Lots of data. Arguably, the most interesting big data projects involve analysing information about people. The big data projects with some of the most valuable applications for companies and public sector organisations alike involve analysing information to make inferences, evaluations and predictions about individuals' preferences, behaviour, performance at work, spending habits, health, location, reliability, the list goes on. The high volume, velocity and variety of the information involved in a big data project means that unless fully anonymised datasets are used, large volumes of personal data will be processed, potentially affecting the privacy rights of the individuals whose data is being processed.

For starters, it is not possible to know whether and how a big data project will impact on the privacy rights of individuals without carrying out an assessment. A privacy impact assessment (PIA) is just that, an assessment of the data flows involved in the project to make sure that the data can be collected, used, processed, stored and shared in the way proposed in the design of the project. If there are any conditions that need to be met or any safeguards that need to be put into place, a PIA will identify them and ensure that the necessary measures are adopted in the project plan. A PIA is also a very useful record that can be used to demonstrate compliance with applicable data protection laws, whichever laws these may be. For these reasons, it is good practice to carry out at least a high level PIA on all projects involving processing of personal data, even when it isn't strictly required by law.

### When is it required

Under the EU General Data Protection Regulation (GDPR), there is a new requirement to carry out a data protection impact assessment (DPIA) where a type of processing is "*likely to result in a high risk*" to individuals. The GDPR applies from the 25 May 2018 to all organisations established in the EU as well as non-EU organisations that offer goods or services to individuals in the EU or monitor individuals in the EU.

Just a word on terminology: a DPIA is the same thing as a privacy impact assessment (PIA) in substance, but the GDPR uses the specific term DPIA when setting out the requirement to do one. For the purposes of this article, we will use the term DPIA to refer to PIAs carried out to meet the specific requirement under the GDPR, and PIA as a more general term that includes DPIAs and other assessments carried out more generally.

When considering whether a proposed project is likely to result in a high risk to individuals triggering the requirement for a DPIA under the GDPR, the following ten criteria should be considered:

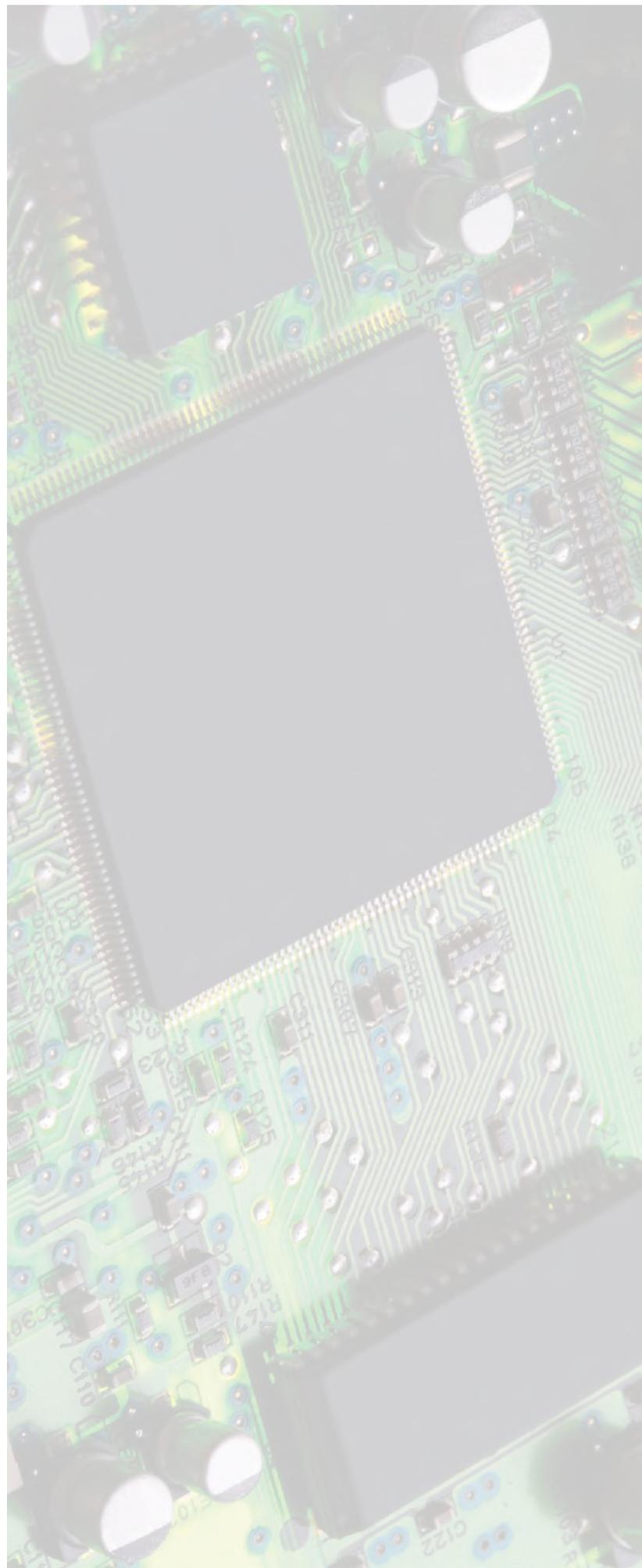
#### 10 Questions: Is the project likely to result in a high risk to individuals?

1. Does the project involve evaluating or scoring individuals, including profiling and predicting aspects about the individual's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements?
2. Does the project involve automated decision-making with legal effects (e.g. terminating a contract, denying access to a statutory benefit, etc.) or similarly significant effects (e.g. denying someone an employment opportunity, access to education, eligibility to credit, access to health services, etc.)?
3. Does the project involve systematic monitoring of individuals used to observe, monitor or control data subjects, including data collected through a systematic monitoring of a publicly accessible area (e.g. footfall traffic analysis in a shopping mall)?
4. Does the project involve processing sensitive personal data? Sensitive personal data includes information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, information about an individual's sex life or sexual orientation and data about criminal convictions and offences.
5. Does the project involve data processed on a large scale, taking into account the number of data subjects concerned, volume of data and the range of different data items being processed, the duration of the processing activity and the geographical extent of the processing activity?
6. Does the project involve datasets that have been matched or combined, for example involving data from different projects set up for different purposes that the individuals involved would not reasonably have expected?
7. Does the project involve processing data concerning vulnerable individuals or individuals in a position of imbalance of power (such as children, the elderly, patients, mentally ill, asylum seekers or employees in the context of human resources management)?
8. Does the project involve a new technological or organisational solutions (such as new Internet of Things devices, use of vision AI such as face recognition or combining existing technologies for innovative solutions)?
9. Does the project involve transferring data across borders outside the European Union?
10. Is the processing of data in the project used to prevent data subjects from exercising a right or using a service or contract? For example, refusing an individual's eligibility to obtain credit, access to a service, entry into a contract or employment?

As a rule of thumb, if the answer is 'yes' to two or more of these questions, the proposed project is likely to present a high risk to the privacy rights of individuals, and so a DPIA will be required to be carried out under the GDPR. Big data projects are likely to meet at least two of the criteria for high risk processing requiring a DPIA in most instances. For example, a project involving gathering information from social media, fitness tracking app usage information, gym access records, and purchasing history from certain retailers to profile individuals' interests, economic status and health to price insurance premiums and offer discounts for certain deals is likely require a DPIA. This is because it would involve (1) evaluation or scoring and (4) sensitive data as well as (6) datasets that have been matched and combined. Another example is a project involving screening CVs and references of job applicants using machine learning algorithms built on an analysis of previously successful candidates. Such a project is also likely to require a DPIA as it would meet criteria (1) evaluation or scoring and (2) automated decision-making.

In some cases, even a project that meets only one of the listed criteria may pose a high risk to the privacy rights of individuals. For example, a smart city project may involve collecting wi-fi signals emitted by mobile phones collected via hotspots throughout the city to understand how many people visit the city, how frequently they visit and how they move around the city. Similar projects may also be carried out at shopping malls, theme parks, music festivals or other venues. Such a project would only involve (3) systematic monitoring of a publicly accessible area, but is likely to result in a high risk to individuals particularly if the movements of the users can be tracked at an individual level, for instance by reference to a device identifier. Given the impact of such monitoring on the individuals' privacy, a DPIA would be required to make sure that safeguards can be identified and put into place.

Even when not required by the law to carry out a DPIA, for instance because the GDPR does not apply to the organisation, it is highly recommended as good practice to at least do a high level review of any big data project to assess the impact of the processing on the privacy of the individuals involved.



## How to carry out a privacy impact assessment

Privacy impact assessments should be carried out at the outset of planning for a project, before any processing takes place. A PIA should be an integral element of the project design and development phase, as the ability to collect and process data lawfully is crucial to the viability of any big data project.

In practice, the PIA is usually carried out through completing three types of documents:

### 1. Preliminary PIA questionnaire.

This document is formulated as a series of questions to obtain information about the project, its purposes and information flows. It is used to make a determination of whether or not a full PIA is required. If it is determined that a full PIA is not required, the responses to the Preliminary PIA questionnaire can be used as a record of the decision not to do a full PIA and a record of processing activities.

**2. PIA Questionnaire.** This document is formulated as series of more detailed questions about the project to obtain the information necessary to complete a full PIA. Once completed, it is used to carry out a full PIA.

**3. PIA Report.** The PIA Report identifies the privacy risks of the project and the measures that need to be taken to safeguard individuals' privacy rights, and contains the following information:

- Description of the envisaged processing operations and purposes of the processing
- Assessment of the necessity and proportionality of the processing
- Assessment of the risks to the rights and freedoms of individuals
- Measures envisaged to address the risks and demonstrate compliance
- Results of any consultation with relevant stakeholders (Data Protection Officer, data protection authorities, data subjects, etc.)

The PIA Report should be kept as a record of the processing activities and as reference for monitoring the implementation of the recommended safeguarding measures.

It is recommended that templates of these three key documents are developed and incorporated into the project development process. Yet, a PIA is more than a document production exercise, and should not be considered a mere formality or box-ticking exercise. The issues identified in a PIA and the recommended measures to safeguard individuals' privacy rights and comply with data protection law needs to be actioned and resolved.

### Key issues likely to be identified in a PIA of a big data project

So far, we've gone over why, when and how privacy impact assessments should be carried out. But what will you find out at the end of the PIA process? This of course depends on the project and the applicable data protection laws.



From a GDPR perspective, however, the following are some of the key issues that can be expected to be identified from a PIA on a big data project:

Issue	Risk to individuals	Recommended safeguards
<p><b>1. Transparency</b> Individuals need to be properly informed about how their personal data will be used</p>	<ul style="list-style-type: none"> <li>In a big data project, there are likely to be complicated information flows with datasets from multiple sources and complex processing activities involving algorithmic and statistic models.</li> <li>Depending on the context of the project, the results from the analysis may reveal unexpected insights into the data that some people might find intrusive or 'creepy'.</li> </ul>	<ul style="list-style-type: none"> <li>It is important that individuals whose data are being used for the project are provided with clear, intelligible information about the how their personal data will be used.</li> <li>The GDPR contains specific requirements about what information needs to be provided to individuals and when it needs to be provided.</li> <li>Measures should be taken to provide appropriate privacy notices to individuals.</li> </ul>
<p><b>2. Lawfulness</b> The processing activity must be lawful, meaning that there must be a lawful ground for processing the personal data and any special conditions must be met if applicable</p>	<ul style="list-style-type: none"> <li>Big data projects are likely to rely on the lawful ground that the processing is in the legitimate interests of the organisation carrying out the project. In such cases, it is important to identify the specific legitimate interests being pursued (e.g. marketing analysis, human resource management, fraud prevention, improved efficiency, etc.) and those interests must not be outweighed by the rights and freedoms of the individual.</li> <li>In some cases, consent from the individual will be required if there is no alternative lawful ground or if a special condition applies, for instance because there is sensitive data involved or there is automated decision-making that has a legal or other similarly significant effect.</li> </ul>	<ul style="list-style-type: none"> <li>The PIA will identify which lawful grounds should be relied on for the particular processing activities at hand.</li> <li>If consent is required, measures will need to be taken to collect valid consent that meets the higher standards for consent under the GDPR.</li> <li>Even if consent is not required, safeguards may need to be put into place to rely on legitimate interests, such as allowing individuals to opt out of the big data project.</li> <li>Appropriate policies and processes will need to be in place to ensure that the project does not experience 'mission creep' where the processing goes beyond what is allowed under the lawful ground being relied on.</li> </ul>

Issue	Risk to individuals	Recommended safeguards
<p><b>3. Purpose limitation</b> Personal data must be collected for specific purposes and used only for those purposes.</p>	<ul style="list-style-type: none"> <li>• Big data projects often take the approach of analysing all of the data that is available, collated from a multitude of diverse sources to create a rich dataset. There may not even be a clear specific purpose at the outset of the project.</li> <li>• This means that personal data may be processed for purposes that are yet unknown and unexpected for the individuals involved. These purposes may also be incompatible with the purposes for which the data was initially collected.</li> </ul>	<ul style="list-style-type: none"> <li>• Make sure that the data used is collected fairly, lawfully and transparently.</li> <li>• Check the privacy notices provided to the individuals at the point of data collection.</li> <li>• Consider whether the analysis is likely to be compatible with the purposes for which the data was originally collected. If not, the individuals will need to be informed.</li> <li>• Consider using anonymised datasets for the initial scoping phase of the project.</li> </ul>
<p><b>4. Individuals' rights</b> Individuals' rights need to be respected and processes must be in place to respond to requests from individuals to exercise their rights.</p>	<ul style="list-style-type: none"> <li>• Individuals have certain rights over their data, subject to local law, including: <ul style="list-style-type: none"> <li>• access</li> <li>• rectification</li> <li>• erasure</li> <li>• restriction of processing</li> <li>• data portability (this right applies only where personal data is processed on the basis of consent or contractual necessity)</li> <li>• objection (where the processing is based on the 'legitimate interests' condition)</li> <li>• certain rights in respect of automated decision-making</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Policies and processes must be in place to respond to requests from individuals to deal with any requests to exercise their rights.</li> <li>• Systems need to be designed so that individuals' rights can be actioned. For instance, systems need to be able to export, delete or rectify data if requested.</li> </ul>

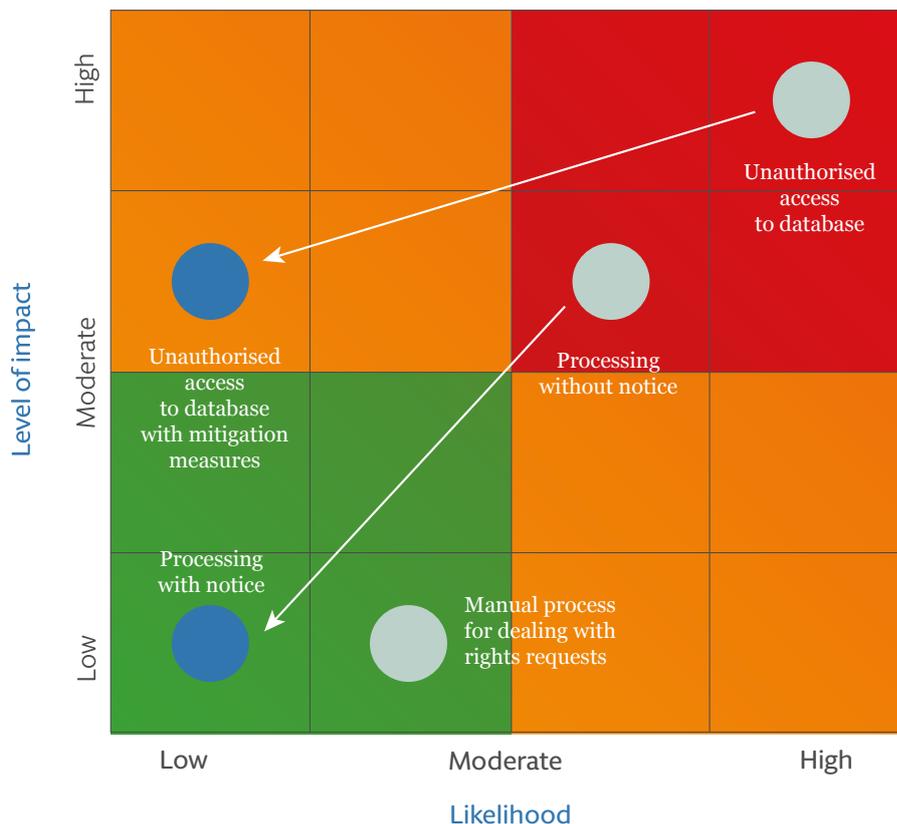
Issue	Risk to individuals	Recommended safeguards
<p><b>5. Security</b> Personal data must be kept securely and adequately protected</p>	<ul style="list-style-type: none"> <li>As big data projects tend to involve large datasets, it is very important to keep this data protected from accidental or malicious loss.</li> <li>This is particularly important when there are multiple organisations (such as companies, academic institutions, public sector bodies, etc.) cooperating to share their data, resources and expertise, so that data is not compromised in storage or in transit at any of the participating organisations.</li> </ul>	<ul style="list-style-type: none"> <li>Technical and organisational security measures must be in place to keep the information secure.</li> <li>Measures such as encryption and pseudonymisation should be adopted and effective processes should be in place to deal with data breaches.</li> <li>If anonymised datasets are used, regular testing should be carried out to ensure that the individuals cannot be re-identified.</li> <li>Contractual safeguards should also be in place between participating organisations to ensure the division of responsibilities are clearly set out</li> </ul>
<p><b>6. Accountability</b> Organisations must be able to demonstrate compliance with data protection obligations</p>	<ul style="list-style-type: none"> <li>In some big data projects, especially those making use of machine learning using unstructured datasets or other innovative analysis methods, there is a risk that the methods for deriving outcomes are opaque, creating a 'black box' effect.</li> <li>This type of processing can pose particular risks for individuals because it is more difficult to demonstrate that the processing has been carried out fairly and lawfully.</li> </ul>	<ul style="list-style-type: none"> <li>Measures should be in place to ensure that algorithms are auditable.</li> <li>A human review of the algorithm should be carried out to ensure that the approach taken is ethical and non-discriminatory. Algorithmic biases that may lead to direct or indirect discrimination on any protected characteristics must be corrected.</li> </ul>

### Making risk-based decisions based on a PIA

Once a PIA has been completed, the next step is to decide how to deal with the risks that have been identified. As discussed above, a number of privacy risks are likely to be identified through a PIA of a big data project. Whilst the key principles and obligations in the GDPR provide a regulatory framework through which privacy risks can be identified, the GDPR is largely silent on what constitutes a "reasonable" level of risk to take on a project and what measures are "appropriate" to mitigate privacy risk. For instance, it is evident that a security breach resulting in unauthorised access to the project database which contains information about a large number of individuals is likely to result in a significant privacy risk to the individuals involved. Yet, what is the "appropriate" security measure to take? And as no solution is ever perfect, when does an organisation know that they have done enough, and that the residual risks are "reasonable" to take? The short answer to these issues is that it depends. It depends on the type of personal data, the categories of data subjects, the processing activities, the systems and algorithms used, the measures and safeguards already adopted, the purposes of the project and the risk tolerance and culture of the organisation in question. The GDPR only tells us that the measures must "*tak[e] into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.*"<sup>1</sup> For data protection by design<sup>2</sup>, and security measures<sup>3</sup>, the GDPR says that measures should also take into account the state of the art and the cost of implementation.

One way to usefully visualise the privacy risks in a project to determine the relative priorities for allocation of resources is through a privacy risk map, which may look like the below:

### Example privacy risk map



In this Example Privacy Risk Map, the various privacy risks associated with a project are evaluated on the basis of the severity of privacy impact on the individuals involved and the organisation and the likelihood of the risks arising. The privacy risk map can also track the change in risk profile once mitigation measures are adopted. For example, the PIA of a big data project may identify a shortcoming in the database security system. If this were the case, there would be a high likelihood of unauthorised access to the database. If such a security breach were to occur, this would result in a significant impact to the individuals as well as the organisation concerned. Therefore, this risk would be mapped on the privacy map in the red upper right hand section as shown, and be flagged as a top priority item for remediation. Mitigation measures would be needed to move the risk downward (lower impact) and to the left (lower likelihood) on the graph. Any risk in the upper right hand section of the graph is likely to be considered unacceptable under any circumstances. On the other hand, the PIA may identify as a risk that the only way the organisation can deal with certain individuals' rights requests is by processing them manually. However, based on previous track record, the organisation does not expect a high level of rights requests and is confident that it can deal with such requests as they come in using existing processes and resources. In this case, the risk would be mapped on the privacy risk map in the lower left hand section as shown, with a lower priority for remediation. Other risks can be mapped on the privacy risk map in a similar way.

Even after privacy risks have been evaluated, mapped and prioritised, there is still the question of deciding what measures are "appropriate" to reduce the level of risk to an acceptable level. A common sense approach to this question would be to balance the costs and efforts of implementing safeguards against its obligations to protect the privacy of the individuals involved. The level of mitigation measures adopted should be proportionate to the likelihood and level of impact of the risk – the bigger and more likely the risk, the more robust the safeguards. That much is obvious, and uncontroversial.

However, measures taken to mitigate risks may be costly. The most significant cost will often be the reduced utility of the data processing brought about by the mitigation measure. This is especially true in big data projects where the obvious mitigation measure – anonymize the data – may significantly reduce the value of the insights derived from the data. To reach an acceptable level of risk, and determine what level of mitigation measures are "appropriate", we contend that a key factor to consider is the underlying purpose and the expected social welfare resulting from the project, and how the mitigation measures may affect that social welfare.

The U.S. Federal Trade Commission ("FTC") has developed a similar methodology to determine whether a data practice is "unfair" and therefore prohibited by Section 5 of the FTC Act. The FTC developed explicit guidelines to help make its methodology for judging "fairness" more transparent and predictable by businesses. A business practice is considered unfair if it causes substantial injury to consumers that consumers cannot reasonably avoid, and the injury is not offset by corresponding consumer benefits. In other words, the practice would be prohibited as unfair if and only if:

$$H - H_A > W_A - W_P$$

Where:

H is the total aggregate consumer harm created by the practice

$H_A$  is the aggregate harm that consumers can reasonably avoid

$W_A$  is the total consumer welfare when the practice is allowed

$W_P$  is the total consumer welfare when the practice is prohibited

How is this formula relevant in the context of assessing privacy risk mitigation measures under the GDPR? To bring this formula to life, let's take two different types of hypothetical big data projects:

- **Project 1:** A visual AI pilot project involving handheld devices carried by visually impaired individuals in a national museum to provide real-time feedback about the exhibition and the people around them
- **Project 2:** A visual AI pilot project involving digital billboards installed in shopping malls that analyse passers-by's fashion trends and shopping bags to display real-time custom advertisements of available products and offers

Both projects involve similar technology (i.e. visual AI) and process similar types of personal data (i.e. biometric information, information about the behaviour of individuals, etc.) about similar categories of data subjects (i.e. individuals in public places) with similar risks to individuals' privacy (i.e. individuals in public places may not wish to be filmed with visual AI technology analysing them). Let us assume that on an initial PIA of both projects, it has been identified as a risk that the individuals who are being filmed and analysed are not given appropriate notice of the processing taking place. If these projects were to proceed without proper notice, the practice would be in breach of the transparency obligations of the GDPR. Yet, when deciding how to provide the notice and accepting any residual risks if a pragmatic solution is adopted, an analysis based on the formula above can be useful, as below:

	$H-H_A$ (total aggregate consumer harm created by the practice) – (aggregate harm that consumers can reasonably avoid)	$W_A-W_P$ (total consumer welfare when the practice is allowed) – (total consumer welfare when the practice is prohibited)
<b>Project 1</b>	<ul style="list-style-type: none"> <li>The harm (H) created by the project proceeding without proper notice would be that individuals visiting the museum may be filmed and analysed through visual AI technology without their knowledge. In particular, the museum may be visited by children. Without proper notice of the processing activities, visitors to the museum will not be able to avoid being subject to the processing or to object to the processing. To avoid the harm, visitors would have to refrain from visiting certain parts of the museum, which is not a reasonable avoidance mechanism. <math>H_A</math> would therefore be zero.</li> </ul>	<ul style="list-style-type: none"> <li>The benefits of the project would be greater accessibility of cultural and educational centres to visually impaired people to encourage them to visit and navigate the premises independently. The success of the pilot programme could be an important precedent for similar programmes in other public places improving access for visually impaired people. If this project were not to proceed, this would limit the way new visual AI technologies could benefit visually impaired people.</li> </ul>
<b>Project 2</b>	<ul style="list-style-type: none"> <li>The harm created by the project proceeding without proper notice would be that individuals visiting the shopping mall may be filmed and analysed through visual AI technology without their knowledge. In particular, the shopping mall may be visited by children. Without proper notice of the processing activities, visitors to the shopping mall will not be able to avoid being subject to the processing or to object to the processing. Let us assume that as in Project 1, <math>H_A</math> would be zero.</li> </ul>	<ul style="list-style-type: none"> <li>The benefits of the project would be more effective on-premise digital billboard marketing for shopping malls. The data collected through the digital billboards can be used to analyse fashion trends, shopping habits and popular brands to maximise the effectiveness of marketing campaigns. The project could also help shopping mall visitors find the products and offers that are more relevant to them effectively. If this project were not to proceed, this could limit the effectiveness of offline in-premise marketing campaigns</li> </ul>

“

As public awareness and interest in big data, artificial intelligence and machine learning heightens, it will become increasingly important to build relationships of trust with the public.

”

The net harm analysis is very similar for both projects: the harm is that visitors could be filmed and analysed without their knowledge, and the harm cannot be easily avoided by visitors in either case. However, the benefits analysis is different. On the one hand, Project 1 has a public policy benefit as it has the potential to improve access to public places for visually impaired people that would have a significant positive impact on their quality of life and opportunity. On the other hand, Project 2 has a commercial benefit that would improve the effectiveness of marketing campaigns and improve profitability of the participating companies.

For both projects, the solution is clear: individuals need to be given notice of the processing so that they can reasonably avoid the harm if they wish. With appropriate notice, the benefits of both projects would outweigh the harm. But given the different benefit profiles of the two projects, it is arguable that the measures that need to be taken to provide this appropriate notice is different, as below:

- For Project 1, it may be sufficient to provide a prominent notice at the entrance of the museum about the project with information about how to get in touch if there are questions or concerns. The handheld devices can also be of a prominent colour, with a light indicating when it is in use, so that it is clear when they are being used. Given the benefits of this project, it is arguable that such measures would be enough to provide a reasonable level of notice.

- For Project 2, a similar approach may not be sufficient. In addition to a notice at the entrance of the malls, additional notices may need to be served at each digital billboard. It may also be a reasonable safeguard to calibrate the digital billboards such that only the people who step inside a clearly delineated space are subject to the analysis and profiling, so that people can easily avoid those spaces if they wish.

To put it simply, given the different societal benefits in the two projects, the level of "appropriate" technical and organisational measures may also be different. Members of the public will be more accepting of such pilot programmes to improve access for visually impaired individuals. Though this doesn't exempt Project 1 from privacy considerations altogether, it means that in practice, people are less likely to object or complain about the processing, which gives more leeway when making risk-based decisions on specific safeguards to be adopted. In contrast, though Project 2 is not without its benefits, people are more likely to view visual AI and profiling for marketing purposes to be more intrusive. Given the high numbers of complaints regulators receive about direct marketing, a pilot programme like Project 2 is likely to result in more complaints and regulatory scrutiny than Project 1. With this in mind, it is advisable to take a more circumspect approach to providing appropriate notices and general data protection compliance for Project 2.

At the end of the day, privacy is an intangible and in most cases immeasurable right. How people feel about privacy is often based on emotions and subjective evaluations about the trade-offs involved. Privacy risks that are acceptable for processing for a certain purpose may not be acceptable for another purpose. Risk mitigations measures which are reasonable for privacy risks in one context may not be appropriate for another context. This is what makes carrying out PIAs so critically important for any project that involves the processing of personal data, and especially big data projects. The PIA is one of the most important tools that organisations have at their disposal to ensure compliance with data protection laws, as it provides a framework for identifying the risks and the specific safeguards to be adopted. The PIA will start with a description of the anticipated benefits associated with the project, both commercial benefits and broader societal benefits. A clear identification of the benefits will help gauge the level of mitigation measures necessary to address each risk. Each mitigation measure should be evaluated based on its effectiveness in reducing the risk, but also based on its impact on the benefits anticipated from the project. A mitigation measure may be extremely effective, but if it destroys half the utility of a big data project, it may be excessive and therefore not "appropriate".

As public awareness and interest in big data, artificial intelligence and machine learning heightens, it will become increasingly important to build relationships of trust with the public. Ensuring that personal data is processed fairly and lawfully, respecting individuals' choices and keeping them informed are crucial for both public acceptance and compliance with evolving data protection laws. The PIA is the key for identifying the specific, practical steps that must be taken to achieve this aim. We suggest that the PIA should clearly identify the benefits associated with a data project so that risk mitigation measures can be evaluated with the benefits of the project in mind.



**Sam Choi**

Associate, London  
T +44 (20) 7296 5756  
sam.choi@hoganlovells.com



**Winston Maxwell**

Partner, Paris  
T +33 1 53 67 48 47  
winston.maxwell@hoganlovells.com

# A blockchain-proof legal department: insights from Bruno Massot – IBM France

Not a day passes without seeing the keyword "blockchain" in our newsfeeds. With artificial intelligence, blockchain is the emerging technology that mesmerizes all sectors and industries. Nowadays, this blockchain madness allows a company to increase its value by 400 percent by simply adding the magic word 'blockchain' in the company name<sup>9</sup>. But is it just a buzzword? To IBM and its legal department, it is not. For four years, IBM has decided to tackle the development of blockchain-based systems and has more than 400 projects underway. A challenge for technical and commercial teams, but also for the legal teams. After a few years of practice as a lawyer and various positions held within the IBM group, Bruno Massot was appointed IBM France's General Counsel in 2013. Within IBM, he is also part of a working group which is, at a global level, dedicated to activities related to blockchain, in order to anticipate the legal questions which arise around its use cases and about which he has agreed to tell us.

## Could you first give us a definition of blockchain?

**Bruno Massot:** If blockchain is especially known to track and secure the exchange of cryptocurrencies like Bitcoin, it is above all a recording system whose content is duplicated simultaneously on several servers, called nodes, and which constitute a network accessible by several participants, without the intervention of any intermediaries or trusted third parties. Blockchain belongs to the wider family of distributed ledger technologies (DLTs). Its main feature consists in preserving in an immutable way the trace of any transaction, financial or not, and more generally of any flow, whether it is data, goods (tangible or intangible) or information.

How does it work? Let's consider one or more events, such as transactions, that are identified and compiled in a block of data, which is authenticated by a digital footprint: a hash. This block is permanently linked to the block that traced the previous events, thus constituting a chain of blocks retracing the sequence of successive events. This allows the development of an immutable and shared register in which this information is recorded.

Another definition element that I believe to be important is the distinction between the public (or permissionless) blockchain and the private (or permissioned) blockchain. In a few words, in the public blockchain, everyone has access to the same data, without the need to identify themselves in a nominative way and the users usually act under a pseudonym. By contrast, in a private blockchain, only a group of selected and identified users are allowed to use it and differentiated accesses may be given as needed.

### Can you give us some examples of blockchain projects that IBM is working on?

Many projects have a goal limited to testing the feasibility of a use case (referred as "proof of concept" or POC) but some of them have gone beyond and have resulted in "minimum viable products" development or even in solutions currently in production.

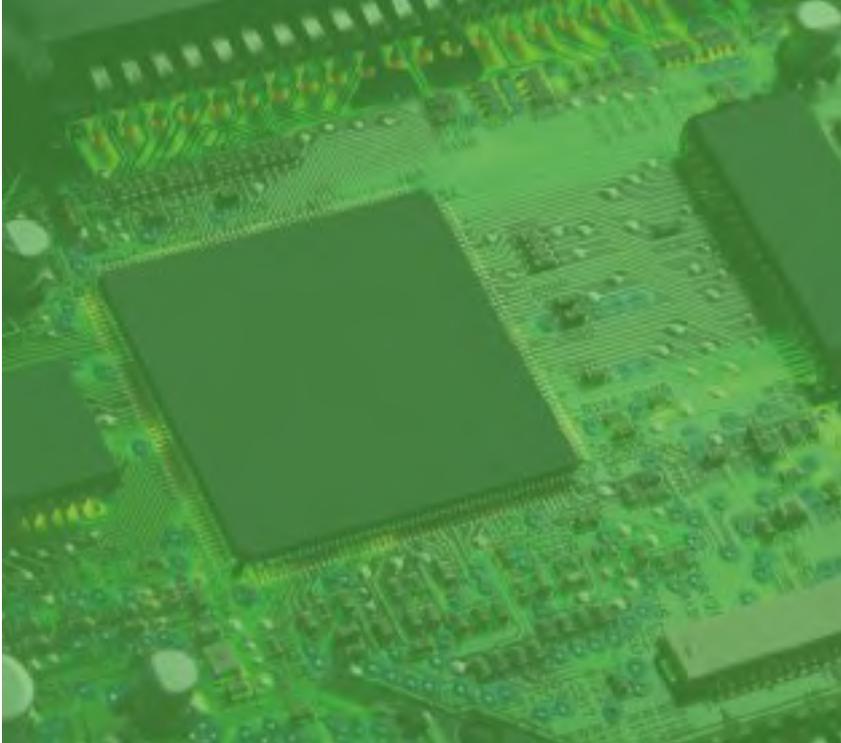
Among the projects that were completed, one was implemented for our own internal needs as part of our financing activities. We noticed that this kind of operation involves a large number of interlocutors – carrier, distributor, financier, builder, etc. – and that at each stage, it requires movement of documents and information. To improve the transfer of this information, we have implemented a blockchain-based system for some partners with whom we carry out large volumes of operations. It allows us to organize, trace and manage document flows, to ensure the contract management, so as to reduce the number of disputes which may occur on documents that did not arrive on time, with latency periods linked to information exchange.

Among the solutions in production, I can also mention a food traceability system implemented in China. It allows tracking the path of pork meat, "from farm to fork". Another system, developed with the company Everledger, allows tracking the production cycle of a diamond, to ensure that it does not have a doubtful origin or that it does not contribute to the financing of illegal activities. Other projects have also been tested in the logistic and financial sectors. For example, we have developed a solution with the shipping company Maersk, which makes it possible to streamline the management of bills of lading to ensure the transparency and security of information flow, especially among the multiple logistic and financing stakeholders (up to 200 for a single product, throughout its global journey to the retail stores) and with regard to customs or tax authorities.

“

Other seemingly classic issues arise in a new light.

”



### How is the involvement of lawyers in blockchain-related projects modified compared to traditional projects?

When assisting a client in the implementation of such a project, the role of the lawyers at IBM remains fairly traditional: assisting sales and technical teams in the contractualization of what the customer expects from us.

Other seemingly classic issues arise in a new light

But we also noted that in-house lawyers are involved earlier, compared to a traditional IT project. It may be explained by the regulatory dimension, which is quite important: blockchain implementation is sometimes contemplated to address a regulatory need, or at least raise an issue that interests the in-house lawyer, particularly concerning the data retention and its dissemination between several actors, notably for evidence purposes.

In the context of POCs, we found it interesting to introduce design thinking workshops, which is an iterative, end-user centric co-creation process. These workshops allow identifying the need and value sought before dealing with the means. In a blockchain-based application, the legal dimension is usually integrated from this stage. Clients' in-house lawyers are more involved in the expression of needs and in the definition of the constraints to be taken into account.

But, as with some other technologies, blockchain raises some issues for which lawyers are well-armed, as regard to ethics, the place of data, and the longer-term trend of the technology which is used by our companies.



### How did you and your team become familiar with this new topic?

We are still in the process of adopting this technology, which requires a clear understanding of the projects we are working on, a careful reading of the literature available on the topic, given that a number of law firms and universities have taken an interest in blockchain. Since Bitcoin is not blockchain itself, it is also about identifying what is specific to cryptocurrency and then moving away from it to focus on the underlying blockchain technology.

To work on blockchain, it remains critical for the lawyer to understand some operational elements and anticipate the legal issues that will arise, contrary to more traditional projects, where it is no longer essential for the lawyer to understand how the Internet works for instance.

At IBM, we are fortunate to have access to people at the forefront on these topics, to explain to us technical concepts that are a little more difficult to grasp. My entire team has been trained to deal with blockchain because I believe this topic to be unavoidable. Forecasts on the use of this technology show that its adoption, and the resulting integration into companies' business models, may take several years. Yet, it is the right momentum to understand it, for us to provide adequate support to our sales and technical teams who are already very active on the subject.

### What legal issues does blockchain raise for your department?

Blockchain raises classic issues related to intellectual property, the mechanism of distribution of roles within a project, etc. Even if answers may be less obvious to provide in the context of a new technology, they do not appear to be radically different.

Other seemingly classic issues arise in a new light. For instance, data protection may raise issues in the context of blockchain, particularly related to the immutability of technology. On the one hand, this immutability is one of the strengths of blockchain. But on the other hand, it raises issues regarding its compatibility with the right to be forgotten, or the need to ensure that personal data are processed for a period appropriate to the purposes in question. The specificity of blockchain is that once the information is stored, it will remain there and cannot be removed. It may be possible to provide a change or a complement in a subsequent block, but the initial block will remain. In public blockchains, this can be a real issue. On the other hand, with private blockchains, on which we usually work, access to the data is one of the elements defined upstream: in such context, this technology can allow better control of data access as this allows, for example,

to limit access to the previous blocks to some people (such as auditors or a supervisory authority) and to combine these limitations with time limits.

One of the biggest differences with traditional IT projects is that we more often face consortiums than with individual companies. As blockchain allows secure exchanges between several stakeholders, we, therefore have to deal with consortiums of different companies, without a single legal personality. We are thus sometimes led to conduct multilateral negotiations, with a set of parties who must coordinate with each other to be properly aligned.



**Bruno Massot**

Directeur Juridique France /  
Senior Counsel France  
IBM Law Department, Europe  
T +33 158 75 34 61  
M +33 684 95 31 10

# A preview of the FTC's role in monitoring broadband markets following the FCC's adoption of the Restoring Internet Freedom Order

Amid the ongoing discussion surrounding “net neutrality,” the FTC’s role in overseeing broadband Internet access service (BIAS) has received increasing scrutiny following the recent passage of the FCC’s *Restoring Internet Freedom Order* (“RIF Order”). Several recent developments indicate that, although the Federal Communications Commission (FCC) will continue to have a shared role in monitoring broadband markets, the Federal Trade Commission (FTC) will take the lead in investigating and bringing enforcement actions against Internet Service Providers (ISPs) for practices that raise anticompetitive concerns. Therefore, commercial stakeholders should pay careful attention to the potential for antitrust enforcement in broadband markets moving forward.

## Background

In 2015, the FCC issued the *Open Internet Order*, which re-categorized BIAS providers as “common carriers” under Title II of the Communications Act. This development is relevant from an antitrust perspective because common carriers are exempt from the FTC’s purview under Section 5(a)(2) of the FTC Act. As a result, the *Open Internet Order* provided the FCC with singular authority to regulate ISPs’ practices related to last mile delivery and network management. In addition, the *Open Internet Order* instituted a series of preemptive conduct rules that explicitly prohibited ISPs from engaging in general categories of practices known as blocking, throttling, and paid prioritization, the latter of which describes a situation in which an ISP directly or indirectly favors certain online traffic in exchange for payment.

“

Commercial stakeholders should pay careful attention to the potential for antitrust enforcement in broadband markets moving forward.

”

Following the change in presidential administrations, the FCC's newly appointed Chairman, Ajit Pai, indicated that the FCC would seek to reclassify BIAS as an "information service" under Title I of the Communications Act, rather than as a "common carrier" service.

### Discussion of the FTC's Enforcement Authority in the Restoring Internet Freedom Order

In support of the FCC's decision to reclassify BIAS as an "information service" and repeal the *Open Internet Order's* conduct rules, the *RIF Order* reinstated a modified version of the "Transparency Rule" adopted by the FCC in 2010.<sup>10</sup> The Transparency Rule specified that BIAS providers must "publicly disclose accurate information regarding the network management practices, performance characteristics, and commercial terms of its broadband Internet access services".<sup>11</sup> The *RIF Order* noted that these disclosure requirements will enable the FCC and FTC "to observe the communications marketplace" while also providing "valuable information to other Internet ecosystem participants".<sup>12</sup> The *RIF Order* then goes on to explain that the Transparency Rule would allow the FTC to serve as an effective "backstop" given the FTC's "broad authority" to enforce antitrust and consumer protection law.<sup>13</sup> The *RIF Order* thereby created a regulatory framework for BIAS that relies on a combination of mandatory disclosures and case-by-case antitrust enforcement.

While the *RIF Order* eliminated the 2015 conduct rules, it approvingly cited to comments submitted by FTC staff that explained that the agency need not demonstrate an ISP has "monopoly power" in a relevant market in order to challenge an ISP's network management practices.<sup>14</sup> The *RIF Order* then explains that the FTC could continue to challenge practices that may be categorized as improper blocking and throttling, as well as certain forms of paid prioritization.<sup>15</sup> With respect to blocking and throttling, the *RIF Order* noted that many of the largest ISPs have committed not to block or throttle legal content in a manner that is inconsistent with their network management practices, which are required to be disclosed under the Transparency Rule.<sup>16</sup> The *RIF Order* indicated that "[t]hese commitments can be enforced by the FTC under Section 5 [of the FTC Act]".<sup>17</sup> Regarding paid prioritization, the *RIF Order* stated that, in a variety of contexts, such arrangements can actually promote economic efficiency and innovation by enabling ISPs to better price services associated with content delivery and network management.<sup>18</sup> However, the *RIF Order* also acknowledged that, under certain limited circumstances, specific forms of paid prioritization, such as an arrangement that favors affiliated content in a way that forecloses customers' access to non-affiliated content, could produce consumer harm and negatively impact competition in a relevant broadband market.<sup>19</sup> For these reasons, the *RIF Order* takes the view that "it is difficult to determine on an *ex ante* basis [that] paid prioritization agreements



“

The FTC is positioned to become the primary agency responsible for reviewing ISP conduct.

”

are anticompetitive” and concludes that “antitrust law, in combination with the [T]ransparency [R]ule. . . is particularly well-suited to addressing any potential or actual anticompetitive harms that may arise from paid prioritization arrangements.”<sup>20</sup>

#### The Allocation of Enforcement Responsibilities under the FTC-FCC Memorandum of Understanding

On December 14, 2017, the FTC and FCC officially signed and adopted a Memorandum of Understanding (“MOU”) that took effect upon the passage of the *RIF Order* that same day.<sup>21</sup> The MOU outlines how the two agencies intend to coordinate their online consumer protection efforts, including oversight and enforcement efforts related to ISPs, and cooperate with each other in monitoring broadband markets.<sup>22</sup>

The MOU generally divides the FCC’s and FTC’s jurisdiction over BIAS as follows:

- **FCC Role in Ensuring ISPs Comply with the Transparency Rule:** The MOU directs the FCC to review, among other things, informal protests submitted by consumers and, where appropriate, take enforcement actions against ISPs that fail to comply with their disclosure obligations or make their disclosures publicly available. The MOU also states that the FCC will monitor broadband markets in order to identify entry barriers.
- **FTC Role in Challenging ISPs for Unfair and Deceptive Practices and Inaccurate Disclosures:** The MOU states that the FTC will review and challenge ISPs for unfair and deceptive practices, including anticompetitive practices related to the provision of BIAS. This authority extends to investigating the accuracy of ISPs’ disclosures while also enabling the FTC to bring enforcement actions against ISPs for specific practices related to their marketing, advertising, and promotional activities that may be found to violate antitrust or consumer protection law.
- **Calls for more exchanges of information and inter-agency cooperation:** The *RIF Order* specifies that the agencies will securely share stakeholder complaints relating to BIAS. Information exchanges between the agencies are therefore subject to policies that require the agencies to protect confidential, personally-identifiable, and non-public information that complainants submit. The *RIF Order* also calls on the agencies to discuss potential investigations against ISPs that could arise under either agency’s jurisdiction, share best practices, and collaborate on consumer and industry outreach efforts.

### Questions Surrounding the FTC's Enforcement Authority

The question of whether the FTC will have the authority to bring enforcement actions as envisioned by the *RIF Order* and the MOU remains open. In particular, on August 26, 2016, the Ninth Circuit dismissed an FTC case against AT&T Mobility for certain throttling practices taken in connection with wireless data services provided to AT&T customers with limited data plans. While the FTC argued that Section 5(a)(2) is “activity-based” and extends only to those activities that are themselves classified as “common carrier” services, the Ninth Circuit ruled that this exemption is “status-based” and extends to any and all activities engaged in by an entity that is classified as a “common carrier,” irrespective of whether the entity’s activities actually being challenged by the FTC under Section 5 are themselves classified as “common carrier” services.<sup>23</sup>

The FTC subsequently filed for appeal and the Ninth Circuit granted rehearing *en banc*, effectively setting aside the panel decision pending review. While this case was pending at the time the *Restoring Internet Freedom Order* was passed, the FCC cited the FTC’s experience in bringing enforcement actions against ISPs (which dates back to 2000), explained that the FCC was not bound by the Ninth Circuit’s holding, and declined to wait for the pending litigation to be resolved in proceeding with the *RIF Order*.<sup>27</sup>

Because an ISP (such as AT&T) may be classified as a “common carrier” with respect to their non-BIAS activities, strict application of the “status-based” test would appear to exempt an ISP’s activities related to BIAS from the FTC’s purview so long as the ISP remains classified as a “common carrier” with respect to their non-BIAS activities. Therefore, resolution of the FTC’s case against AT&T Mobility is likely to have a material effect on the FCC’s and FTC’s ability to carry out the terms of the MOU.

## Conclusion

The *RIF Order* and MOU mark an important policy shift in the regulation of broadband markets. Important questions remain with respect to the specific practices the FTC might seek to address in consumer protection or antitrust cases brought under Section 5 as well as the scope of the FTC's legal authority in light of ongoing challenges to its jurisdiction over BIAS. Nevertheless, the terms of the MOU signal that the FTC is positioned to become the primary agency responsible for reviewing ISP conduct and would have broad discretion to challenge ISP practices related to the provision of BIAS that can result in consumer harm.

---



**Logan Breed**

Partner, Washington D.C.

T +1 202 637 6407

logan.breed@hoganlovells.com



**Trey Hanbury**

Partner, Washington D.C.

T +1 202 637 5534

trey.hanbury@hoganlovells.com

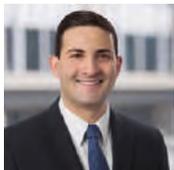


**Alexander Maltas**

Partner, Washington D.C.

T +1 202 637 5651

alexander.maltas@hoganlovells.com



**Daniel Graulich**

Associate, Washington D.C.

T +1 202 637 4828

daniel.graulich@hoganlovells.com

# Tech M&A: the view from the Valley

Market-leading merger & acquisition partners Rick Climan, Keith Flaum, and Jane Ross, and IP & Technology Transactions partner John Brockland recently joined Hogan Lovells' global corporate team. Highly regarded in Silicon Valley and around the world, Climan, Flaum, Ross, and Brockland have worked together for nearly 20 years. Over that period, the team has handled some of the most significant transactions in the technology and life sciences sectors, having worked with companies such as Adobe, Ant Financial, Applied Materials, eBay, Facebook, Gilead Sciences, Intel, Jazz Pharmaceuticals, Marvell Technology, Oracle, Qorvo, Synopsys, and Walmart ecommerce. The Silicon Valley team recently joined Washington, DC-based communications partner Trey Hanbury for a discussion about technology transactions and life in the Valley.

**Trey Hanbury:** I will start with a confession. We in Washington, DC think that the world revolves around us, but business is clearly bigger than the merger review process administered in Washington, DC. Mergers are the result of a series of business decisions made over a period of years in response to discrete market conditions. But – despite expectations of a merger frenzy after the election – we have not seen that much M&A activity. Is the United States really open for business?

**Rick Climan:** There is uncertainty in the US M&A marketplace right now, at least in certain sectors. M&A dealmakers are not sure what to expect. We expected the new administration to be receptive to mergers, but given what's going on in Washington, we just don't know. Is merger review going to continue to be based on traditional antitrust analysis, or is there going to be a new component [of job creation] on top of that? The uncertainty around the scope and nature of regulatory review, coupled with vacancies in key positions in regulatory agencies, may be holding some buyers back because they don't want to be the test cases.

**Keith Flaum:** I would add China to the equation. As you know, the U.S. Government sees potential national security issues with Chinese buyers – particularly in certain sensitive areas, such as the semiconductor space. People thought China was going to be a big driver of M&A activity – but I'm not sure that will be the case in the short term.

**Climan:** Some folks in Washington, DC may be focusing closely on antitrust/competition policy, but that's just part of the picture. There are other regulatory regimes that can negatively impact M&A activity even while the antitrust climate appears relatively open to big mergers.

CFIUS is a perfect example. Combine CFIUS review [in the United States] with the fact that China has been imposing regulations of its own restricting the outflow of capital. Together, these types of measures have made US acquisitions by China-based buyers much more difficult than they were in 2016. 2016 was a watershed year for acquisitions by China-based buyers in the U.S., but the pace of that activity is slowing down considerably right now.

**Hanbury:** And that slowdown is a result of the new regulatory environment?

**Climan:** It is a combination of the new regulatory environments in both the U.S. and China.

**Jane Ross:** Regulations in China are slowing down global M&A. So, the slowdown is not necessarily only impacting the U.S., although that's where a lot of their investments were being made.

**Climan:** We in Silicon Valley tend to pay a lot of attention to the factors driving technology M&A in particular. I think there are four drivers of tech M&A. One is the appetite of domestic strategic acquirers in the technology sector for growth by acquisition. Another is the appetite of foreign strategic acquirers. The third is the private equity sector, which has become, over the years, a major player in technology M&A. And the fourth is the growth aspirations of non-technology companies that are either themselves morphing into technology companies or are looking to expand their digital footprint. This includes both auto companies and retailers -- e-commerce is the name of the game for traditional retailers looking to expand their online presence.

**John Brockland:** That's right. We see companies that haven't been seen historically as tech companies trying to position themselves as [tech companies], for example, by emphasizing in their commercials that their employees are no longer engineers or scientists, but coders and software engineers.

**Climan:** John, why do you think these companies think it's so important for the public to know they are changing into technology companies?

**Brockland:** It could be they are trying to advertise to people who are potential employees. It also could be that they are trying to change their image, because image can impact valuation. The valuation multiples for technology companies are often higher than for non-tech companies, and the forward thinking image that they have is much more exciting.

**Hanbury:** But not all of that [technology acquisition activity] has seemed to amount to much. Established companies acquire tech companies and then they seem to go into their drawer and the established company remains the same company it was before. Where are the synergies there from these acquisitions? What is an established retailer or an established manufacturer going to do with the robotics firm, or how does that marry up [their established business] with some of their far flung investments?

“

Regulations in China are slowing down global M&A.

”



**Brockland:** It takes time, right? I think some technology investments have a pretty long time horizon. Ten years ago if you would have talked about drones or autonomous driving, you would have been laughed out of the room. Now they are part of everyday conversation.

**Climan:** In tech, historically, valuations have been a reflection of projected growth. All the way back to the early days of tech, even before the bursting of the tech bubble [in 2000], there were companies with huge valuations that had not yet become profitable. In some cases, they did not even have meaningful current revenues. As a matter of fact, private equity firms originally shied away from the tech sector because they rely on debt -- leverage -- to generate

returns. It was difficult to pile debt on to certain types of tech companies -- notably software companies -- because those companies didn't have the hard tangible assets that could serve as security for debt. And they didn't have the stable cash flow needed to service that debt. So, in those early days, when banks were reluctant to take a security interest in something as amorphous as software and many tech companies were not yet profitable, prospective financial buyers instead looked closely at growth forecasts. Private equity firms would essentially use growth as a surrogate for leverage, and a good growth story could drive investor returns just as well as layering lots of debt on a deal.

“

Private equity has become over the years a major player in technology M&A activity.

”



“

For people in the start-up world it's almost like a badge of honor if you have started and failed.

”

It's also important to recognize that the valuation metrics used by buyers and their financial advisors to value tech companies are not necessarily the same as those traditionally used in “old economy” sectors. Corporate development and investment banking professionals who focus on “old economy” companies are generally focused on bottom-line oriented valuation metrics, such as cash flow multiples. But for the past 20 years or so, tech bankers have been looking at other metrics as well. Some of these other metrics have been employee-focused, such as “dollars per employee,” “dollars per PhD” and “dollars per engineer.” Let's face it, the most important assets of technology companies aren't factories or other “bricks and mortar” assets; they are human resources and technology assets, neither of which show up on a balance sheet. Other tech-centric valuation metrics -- such as “dollars per eyeball” and “dollars per click” -- focus on the user base. You can't justify some of the incredible valuations we're seeing today in the tech world by relying solely on traditional financial metrics. You have to take into account the tremendous synergies that a large user base can generate.

**Hanbury:** Is there a dichotomy between networks and platforms when it comes to valuing tech assets? Value can be created in all kind of places, but where do you see opportunities in the sector? Is it the edge or is it the network itself?

**Brockland:** It's really not one or the other. It's definitely both. I think the successful companies might be the ones with the platforms and the networks. So you have a company like Facebook or like GE that has a fantastic network or platform, and they're buying this really cool technology and figuring out how to use that technology to expand their revenue, platform, etc.

**Hanbury:** We'll never be tech visionaries (otherwise we wouldn't be lawyers!), but if you are looking at global investment patterns, and you are thinking where the money is coming from, and where companies are going, and where they are looking for acquisitions, is Silicon Valley still the right place to be? Should we be moving to China? Or Frankfurt? If you were trying to start a utopian tech hub of the new generation, should it matter whether you are in the U.K., or Japan, or Germany, or DC? What is your short list of critical elements that you need for a technology hub – and you can't say a good climate!

**Climan:** I do need to say climate. Don't minimize the importance of fantastic weather.

**Hanbury:** Okay, but weather is not enough. What is special about Silicon Valley? Is it a unique mix of risk capital? Is it educated people? Is it mobility?

**Flaum:** There is no other place like Silicon Valley. There is a reason why everybody comes here. There is a combination of free market, rule of law, property rights, stable government and access to capital. There is something like magic. There is the right combination of factors: the right town and the right kind of people. You just walk around in Palo Alto and you see stuff happening and I don't think that kind of stuff happens anywhere else. You think about the biggest companies of the world...Google, Apple, Intel and they are all here and they throw off a ton of talent and a ton of money that nurtures new companies, which grow and then throw off a ton of talent and a ton of money. There is no other place that has that.

**Climan:** But Keith, why can't New York replicate this? Why can't the Dulles corridor replicate this? Why can't Austin replicate this? Colorado? Why Silicon Valley?

**Flaum:** I think it is talent and access to the talent pool.

**Climan:** But why is the talent pool here?

**Flaum:** People come here because of what's already here.

**Climan:** So, it's a first mover's advantage. There has to be, to a certain extent, a first mover advantage.

**Hanbury:** Why aren't other cities popping up and displacing Silicon Valley?

**Climan:** Silicon Valley has Stanford, and UC Berkeley is close by. There aren't many locations where you can find two such preeminent educational institutions so close together.

**Brockland:** It's a combination of all those things. You've got the first mover advantage. You've got the universities. You've got the money. You've got the people prepared to risk money too.

**Flaum:** I also think that there is a culture that promotes risk taking.

**Hanbury:** What if a client is looking for risk capital in Silicon Valley. What advice would you give them? How do you access that? Is it about business plan; is it about the presentation?



**Brockland:** It's the networking.

**Ross:** Yes, it's your connections.

**Brockland:** I have talked to start-ups, some friends of mine that wanted to get introductions, and I would introduce them to somebody, and I may not give them what they expect, but I can get introduced to someone who does that.

**Hanbury:** So, it winds up being a small community?

**Brockland:** Yes, and I like it because it is also a very mobile community. People have been moving around from company to company.

**Climan:** The mobility here is remarkable. One of the factors some people say has promoted Silicon Valley's rise as a tech and innovation hub is that California law actually favors employee mobility in ways that other states' laws do not.

**Ross:** That's probably true. Having access to more employees is possible because [the employees] are not weighed down by non-competition agreements (which are less likely to stand up under California law). And if you are looking at the US versus the rest of the world, the lack of restrictive regulations around employees here is important.

**Brockland:** Silicon Valley has a history of success. Entrepreneurs just look at the companies that have been successful here and they want to come here because there might be a better shot at being successful. Singapore doesn't have it. New York doesn't have it. DC doesn't have it.

**Flaum:** It's about the free spirit. The openness of the community. The acceptance of differences – you can do what you want to do here, which is what free enterprise is all about.

*Interview has been edited and condensed for publication.*



**John Brockland**  
Partner, San Francisco  
T +1 415 374 2308  
john.brockland@hoganlovells.com



**Trey Hanbury**  
Partner, Washington  
T +1 202 637 5534  
trey.hanbury@hoganlovells.com



**Rick Climan**  
Partner, Silicon Valley  
T +1 650 463. 4074  
richard.climan@hoganlovells.com



**Jane Ross**  
Partner, Silicon Valley  
T +1 650 463 4054  
jane.ross@hoganlovells.com



**Keith Flaum**  
Partner, Silicon Valley  
T +1 650 463. 4084  
keith.flaum@hoganlovells.com

# The new European framework on the free flow of non-personal data

On 13 September 2017, the European Commission published its proposal for a *Regulation on a framework for the free flow of non-personal data*<sup>25</sup>. The Commission hereby aims to facilitate the cross border data flow within the European Union and includes new provisions for data storage and processing services (e.g. cloud services providers). The proposal that purely deals with non-personal data is part of the large-scale Strategy for a Digital Single Market. Just in time for the turn of the year, the European Council took a stand on the Commission's proposal and published a revised version of the draft<sup>26</sup>.

Nils Rauer and Andreas Doser outline the key aspects of the proposed regulation and take a sneak preview on the practical challenges for businesses.

## DSM – The big picture

Back in May 2015, the European Commission announced its Strategy for a Digital Single Market. The overall aim was to create and implement a uniform and fairly homogeneous market place on a pan-European basis, particularly for the Internet. The goal of an internal market within the EU was by no means a new idea in 2015. In 1982, the European Court of Justice defined the overall aim of bringing about a market that *"involves the elimination of all obstacles to intra-Community trade in order to merge the national markets into a single market bringing about conditions as close as possible to those of a genuine internal market."*<sup>24</sup> Of course, the judges back then did not have the digital market in mind but were focused on the analogue world.

However, the concept of an internal market as set out in Article 26 TFEU does not stop at the front porch of the Internet. Trade and communication are digital now. This is why phenomena such as geo-blocking, domestic access restrictions and territorial data localisation are perceived as unreasonable obstacles to a barrier-free Internet within the EU.

Over the past three years we have seen plenty of consultations, impact assessments and proposed legislation – partly regulations, partly directives – initiated by the Commission. Some of the initiatives have been enacted already. A good example is Regulation 2017/1128 on cross-border portability of online content services in the internal market, which will take effect from 1 April 2018. The proposed regulation regarding the free flow of non-personal data will be yet another important cornerstone in the course of implementing the Digital Single Market.

## The need for regulation

One of the current issues that many companies are facing is the shortcoming in regards to the mobility of data within the EU. There are major obstacles such as national data localisation restrictions (e.g. for the financial and health industries), a lack of trust in cross-border data storage and processing and difficulties in switching from one online service provider to another because of so-called vendor lock-in practices.

In 2015, the Commission released its first consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy. This was followed by a second consultation on building a European data economy in 2017. No less than 61.9% of stakeholders stated that data localisation restrictions within the EU should be removed. The call for effective measures allowing for cross-cutting free movement of data and the creation of an environment with legal certainty was clearly articulated. Business drivers such as a level playing field, adequate data mobility, the cutting back of data localisation requirements, market conditions allowing for simple ways to switch providers and the porting of data on a cross-border basis and – above all – the need for adequate data security were identified.

It is predicted that in 2020, a fully functioning EU data market could potentially amount to more than € 106 billion. In its latest press release, the European Council estimated that removing data localisation restrictions could allow for "*the data economy to reach its full potential and double its value to 4% of European GDP*" within the next two to three years.

In light of this potential and in consideration of the impact assessment the Commission proposed a draft Regulation on a framework for the free flow of non-personal data that we will look at now.

“

It is predicted that in 2020, a fully functioning EU data market could potentially amount to more than € 106 billion.

”

“

One of the current issues that many companies are facing is the shortcoming in regards to the mobility of data within the EU.

”

”

### Scope of the Regulation

It is important to note that the proposed Regulation does not touch upon personal data. Personal data meaning any information relating to an identified or identifiable natural person is, in the first place, subject to the new General Data Protection Regulation 2016/679 (GDPR) which will apply from 25 May 2018. Here, we talk about non-personal data only.

The provisions of the proposed Regulation shall apply to services relating to the storage or other processing of electronic data. Both terms are to be understood in a broad sense, encompassing the usage of all types of IT systems, no matter whether they are located on the premises of the user or outsourced to a data storage or other processing service provider. The various forms and manifestations such as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) shall be covered.

According to Article 2(1) there is no ultimate need to have an establishment within the EU in order to fall within the scope of application. Rather, the provision of a service to users residing or having an establishment in the EU will suffice. Of course, if the service is carried out by a natural or legal person residing or having an establishment in the EU for its own needs, the provisions of the new Regulation will have to be obeyed.

### Core elements

The draft Regulation as proposed by the Commission is fairly straightforward and concise in its structure. In total, 30 recitals are followed by ten articles. The core provision is without doubt Article 4(1). According to this article, the location of data for storage or other processing within the Union shall not be restricted to the territory of a specific Member State, and storage or other processing in any other Member State shall not be prohibited or restricted, unless it is justified on grounds of public security. Article 4(2) obliges the Member States to notify to the Commission of any draft act which introduces a new data localisation requirement or makes changes to an existing data localisation requirement. In other words, the Commission wishes to keep track of anything that could hamper the free flow of non-personal data.

What will impact the domestic law-making process even more is the obligation set out in Article 4(3) that within twelve months after the application of the Regulation, Member States must ensure that any conflicting laws are repealed. Member States shall make the details of any such data localisation requirements applicable in their territory publicly available online via a single information point which they must keep up-to-date. In other words, Member States are required to become active immediately after the final wording is agreed given the common period of time bills have to climb through the legislative process.

On various occasions, the Commission has emphasized that the powers of competent authorities to request and receive access to data for regulatory control purposes, such as for inspection and audit, must remain unaffected despite the risk that the data at issue might end up being stored and/or processed abroad. Accordingly, Article 5 explicitly stresses the need for data availability. The competent authorities must be able to retain cross-border access to the relevant data. Where a competent authority has exhausted all applicable means to obtain access to the data, it may request the assistance of a competent authority in another Member State. Article 7 provides procedural guidance as to how such requests shall be dealt with (the cooperation mechanism).

However, data access for regulatory control purposes is nothing new for regulated businesses. For instance, outsourcing in the financial services industry already requires that regulators are in a position to request information from the outsourcing provider. This applies even if the outsourcing provider is not regulated and/or does not conduct its activities in the regulator's territory. It is to be expected that the new provisions for data access, in particular the new cooperation mechanism, have the potential to increase regulatory oversight. This is highly relevant as more and more information is stored by cloud service providers and regulatory supervision depends on appropriate tools to address the new outsourcing landscape.



“

The Commission wishes to keep track of anything that could hamper the free flow of non-personal data.

”

### Self-regulation

The Commission, however, does not place its bet only on top-down regulation. Rather, the facilitation of self-regulation is an equal part of the concept as can be seen in Article 6 of the draft regulation. As mentioned above, it is the aim to ease and enable switching between different online service providers as regards the storage or other processing of non-personal data. In this context, the Commission encourages and facilitates the development of self-regulatory codes of conduct at EU-level. Guidelines are to be defined and best practices developed.

Professional users of such services shall be equipped with sufficiently detailed, clear and transparent information before a contract for data storage and processing is concluded. This information shall, *inter alia*, include: (1) the processes, technical requirements, timeframes and charges that apply in case a professional user wants to switch to another provider or port data back to its own IT systems, and (2) the operational requirements to switch or port data in a structured, commonly used and machine-readable format allowing sufficient time for the user to switch or port the data.

### Free Flow of Data Committee

According to Article 8 of the draft regulation, a new Free Flow of Data Committee shall be established to assist the Commission in its endeavours to bring about a true free flow of non-personal data within the Digital Single Market.

### Practical impact

It goes without saying that the free flow of data is and must be a core element and a cornerstone of a fully functioning internal market. Particularly in the digital world, data is an asset of great value. Thus, the overall aim the Commission is pursuing is beyond question. The "tricky" part will be the implementation. For example, the exemption referred to in Article 4(1), i.e. "*unless it is justified on grounds of public security*" is open to interpretation. Of course, guidance can be drawn from previous case law and approved administrative practice as to what determines "*public security*". However, stakeholders and particularly service providers falling within the scope of the new Law will inevitably be confronted with differing views as to what obstacles may be deemed justified on the grounds of public security.

Despite this reservation, the regulation will certainly contribute to a more liberal flow of non-personal data which in consequence will make life easier for companies that depend on service providers that take care of the storage and processing of their data. Not only major international companies but also small and medium-sized enterprises will benefit. At the receiving end, we may thus expect a broadening of options.

Service providers will also benefit from the free flow of non-personal data. They will be able to spread their potential customer base across the EU. Since the location for the storage and processing can be freely chosen, they can expand their offering as far as the Digital Single Market goes. However, service providers will need to review their standard contracts first making sure that the provisions are compliant with the new law. In particular, the new information obligations need to be considered with adequate diligence. For, it may already be anticipated that the right scope and depth of information to be provided to the professional customer will give rise to disputes and litigation. For the time being, it is hoped that the codes of conduct the Commission has requested will provide adequate detail on the data porting conditions which need to be made available to the professional users in advance.

### The Outlook for 2018

With the Commission having put forward the initial draft, it is now for the Council and the Parliament to form their positions and to agree on the final text before the Regulation can enter into force. Whilst the Parliament has not yet adopted its position, the Council published its comments and suggested amendments on 19 December 2017. The Council did so with a clear expectation that all three co-legislators may reach an agreement "*on this priority dossier*" by June 2018.

Amongst the aspects stressed by the Council are unresolved questions around data ownership and appropriate mechanisms for determining liability. Also, the term data "processing" shall be defined most broadly as "*any operation or set of operations which is performed on data or on sets of data in electronic format, whether or not by automated means, such as collection, recording, organisation,*

*structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*".

The twelve-month period for eliminating domestic obstacles to the free flow of data has been extended to two years. Article 5(3a) shall hold additional provisions on sanctions imposed in the case of failure to comply with an obligation to provide data to the competent authority. Also, the Council stresses the need to develop certification schemes for data processing products and services for professional users, taking into account established national or international norms, facilitating the comparability of these products and services. And, the Council does not see the ultimate need for the Free Flow of Data Committee as suggested by the Commission.

“

The free flow of data is and must be a core element and a cornerstone of a fully functioning internal market.

”

All in all, the changes proposed by the Council do not seem so substantial in nature as to deem unrealistic the anticipated end date of discussions in June. Still, we are waiting on comments from the European Parliament.

*This article was first published in Digital Business Lawyer in February 2018.*

---



**Nils Rauer**

Partner, Frankfurt

T +49 69 96236 334

[nils.rauer@hoganlovells.com](mailto:nils.rauer@hoganlovells.com)



**Andreas Doser**

Associate, Frankfurt

T +49 69 96236 445

[andreas.doser@hoganlovells.com](mailto:andreas.doser@hoganlovells.com)

# Evolving landscape for international cloud providers in China: why US technology giants are pairing up with local partners

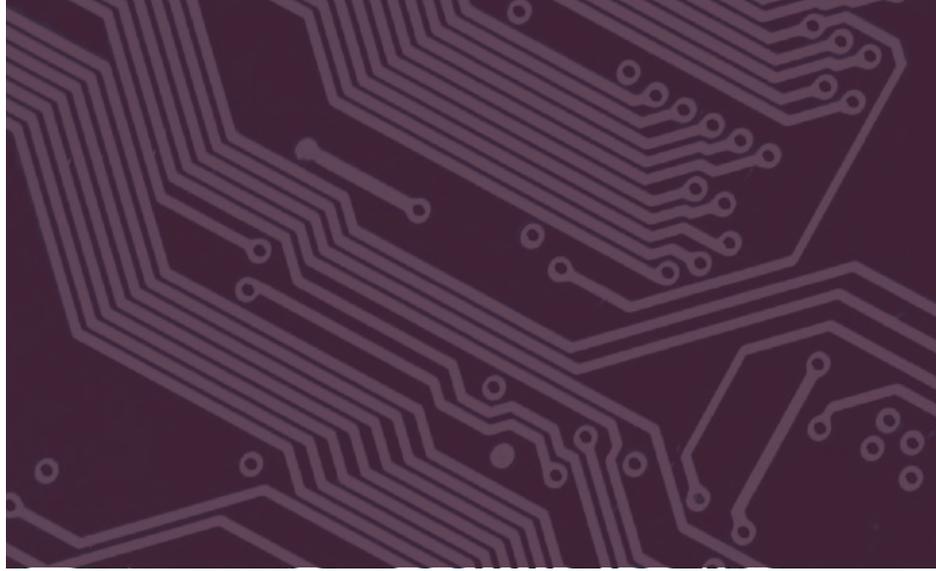
Foreign investment in cloud services is heavily restricted in China. For years, international cloud operators have been struggling to identify structures that address regulatory concerns, but at the same time enable a service delivery model that is consistent with international offerings. Teaming up with Chinese companies is not something new, but it has become a more prominent feature in the cloud space following certain regulatory developments in 2017, notably new licensing requirements issued by the Ministry of Industry and Information Technology ("MIIT"), China's telecommunications industry and internet regulator, as well as the implementation of PRC Cyber Security Law (the "Cyber Security Law").

In the past few months, multiple US technology companies have announced their partnerships with Chinese cloud license holders, naming such Chinese partners as "operators" of their cloud services in China. These cross-border partnerships represent the latest trend in China's cloud industry. This note examines how these US-based technology giants are structuring their China service delivery models, which may provide guidance to others that are looking to enter the Chinese cloud services market, a market which is expected to grow 30% year on year for the next five years, with a value exceeding USD 100 billion by 2020.

“

The Chinese cloud services market is expected to grow 30% year on year for the next five years.

”

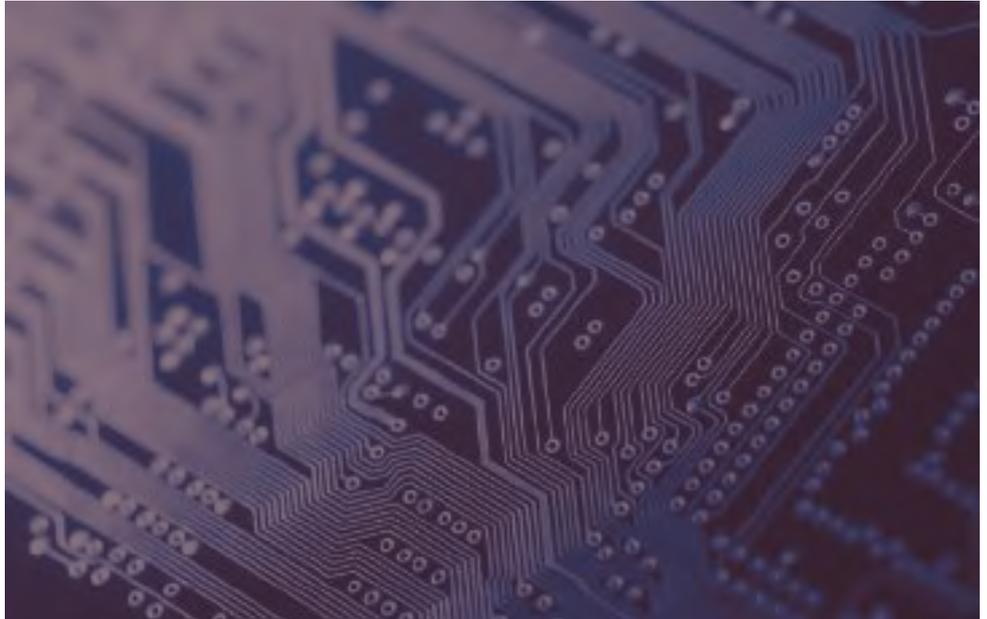


### Licensing requirements for cloud operators in China

To understand this somewhat challenging area and to put it into context, you have to go back to China's liberalisation commitment in this sector when it joined the World Trade Organisation ("WTO"). The resulting commitments allowed foreign investment of up to 50% in Value-Added Telecoms Services ("VATS") and up to 49% in Basic Telecoms Services ("BTS"). However, what is less well understood is that when the section in the WTO accession schedule setting out China's sector-by-sector commitments on VATS (which reads "Value-added telecoms services, including the following [...]" and then lists certain VATS services) was being negotiated, those on the other side of the negotiating table to China interpreted "including" to be the lawyer's "including, without limitation", while MIIT has consistently taken the view that "including" means "namely", so China has no obligation to liberalise any sector not expressly included in the WTO text. Internet Data Centres ("IDC") are classified as a VATS, but are notably absent from the WTO schedule. Hence as far as MIIT is concerned,

there is no commitment to open up this sector to foreign investment. The classification of services into VATS and BTS is set out in the Catalogue for the Classification of Telecoms Services, the latest iteration of which took effect on March 1, 2016 (the "Telecom Catalogue").

Operating cloud services in China generally requires a VATS business operating permit (a "Permit") issued by the MIIT, although there is some debate over whether certain elements of Software-as-a-Service ("SaaS") models require a VATS Permit. A Permit is clearly required for IDC services, a category more meant to cover the hardware aspects of cloud services, in particular the operation of Internet data centers. Beginning March 1, 2016, a separate license was, *de facto* required for Internet Resource Collaboration ("IRC") services, which is set out as a subset of IDC in the Telecoms Catalogue. MIIT has confirmed that this sub-category under IDC covers "cloud services", in the draft Circular on Regulating Business Activities in the Cloud Services Market, issued for public comment in November 2016 ("Draft Cloud Circular"). Please refer to the



detailed discussion of this circular in our client note of January 2017 (see our briefing <http://www.hoganlovells.com/en/publications/draft-legislation-to-affect-china-cloud-services-market-access>).

"Cloud services" were not defined in the Draft Cloud Circular, and may, based on recent market practices, be broadly interpreted to cover three types of services: Infrastructure-as-a-Service ("IaaS"), Platform-as-a-Service ("PaaS") and SaaS. Based on a circular issued by MIIT in January 2017 ("2017 Circular")<sup>28</sup>, cloud businesses established after March 1, 2016 must now obtain an IRC Permit as well as an IDC Permit before going into operation. Cloud businesses with IDC Permits that were operational prior to March 1, 2016 (subject to a notice requirement) had until December 31, 2017 to obtain an IRC Permit in addition, failing which they had to cease engaging in the business.

On January 12, 2018, MIIT issued another circular to reconfirm its position on the requirement for an IRC Permit to engage in cloud business, together with a list of more than 100 companies that have obtained IRC Permits ("IRC License Holders List"), including major Chinese cloud players such as Alibaba and Tencent, as well as local partners of overseas cloud operators, as well as listing those who did not requalify for an IRC Permit.

#### **Foreign participation in cloud services**

As noted above, MIIT takes the view that IDC, and hence by extension IRC, services are not open to foreign investment, and by making IRC a subset of IDC in the Telecoms Catalogue, MIIT effectively made IRC off-limits to foreign investment as well, thereby severely limiting direct equity participation options in the cloud space. There are, however, several potential options that foreign investors can consider when seeking to participate in the cloud space in China. None of these are a panacea and each has

its own pros and cons. Sometimes it may be necessary to mix and match.

Investing through a Hong Kong entity qualified under the Mainland China / Hong Kong Closer Economic Partnership Arrangement ("CEPA")

In strict legal terms, this is the only option for foreign investors to access the Chinese cloud market (primarily IDC as it does not expressly cover IRC) through equity ownership. Under the relevant rules, a CEPA-qualified Hong Kong service provider entity is allowed to establish an equity joint venture with a local Chinese company to engage in IDC business, with the level of Hong Kong ownership capped at 50%. The ownership of Hong Kong companies is not subject to foreign investment restrictions in this sector, meaning that the Hong Kong joint venture partner can be 100% foreign-owned. However, the arrangements remain subject to approval by MIIT, which in practice is not always supportive of equity joint

ventures based on a CEPA arrangement, and, consistent with its restrictive interpretation of China's WTO commitments, has interpreted CEPA as only applying to investors where the ultimate shareholder is from Hong Kong, notwithstanding the fact that this restriction is not set out in CEPA itself.

### VIE structures

The well-known variable interest entity ("VIE") structure typically involves a foreign investor entering into a series of contractual arrangements with a Chinese VATS Permit holder that enables the foreign entity to exercise effective control over the licensed business, and seeks to achieve an equity-like return in a sector restricted to foreign investment. VIE structures are popular in industry sectors restricted for foreign investment, including the telecoms and internet sectors, as well as those where in many cases foreign participation is prohibited, such as many media-related sectors, but do involve substantial risks to foreign investors.

Essentially, the foreign investors have to control the nominee shareholders that own the domestic capital VATS Permit holder. If these nominees turn against the foreign investor and claim outright ownership, they may use, among others, threats of reporting the VIE structure to the regulators because the structure has never been expressly recognized by the Chinese government. Indeed some recent arbitration cases resulted in it being successfully challenged on the basis it was a circumvention of the requirement for the foreign investor to obtain a VATS Permit (with MIIT approval) through a foreign-invested enterprise in China.

In February 2015, the PRC Ministry of Commerce proposed a draft Foreign Investment Law, in which it cast doubt on the legality and sustainability of VIE structures involving control by a foreign investor in restricted sectors (such as all telecoms/internet sectors, including IDC/IRC). This could have a far-reaching impact on many VIEs in China, resulting in challenges for those who have made use of it. However, this proposal has not yet been made law, and there is some expectation that there will be some form of grandfathering or transition for existing VIE structures, as billions of dollars have been invested in PRC businesses through VIE structures, with the businesses listed in Hong Kong and the US. Expectation is not always the same as what transpires in practice, as those who watched the unwinding of the predecessor Chinese-Chinese-Foreign structures can bear witness. The difference this time around is the personal fortunes of many Chinese entrepreneurs are in the mix too. Notwithstanding the well-known risks, *faute de mieux* the VIE structure is still the most commonly used structure for foreign investors to enter restricted sectors in China.



“

Multiple US technology companies have announced their partnerships with Chinese cloud license holders.

”

However, MIIT appears to take the view that cloud and IDC services are too sensitive to be controlled by foreign investors through VIE structures, and so the apparent administrative tolerance for VIE structures in other restricted sectors does not generally extend to this space. In practice, MIIT may exert pressure on the foreign investor's Chinese partner or VATS Permit holder to remove control elements that are viewed as too aggressive. As things stand now, a full-on version of the VIE structure as seen in the venture capital world in other telecoms/Internet sectors, for example, seems to be a non-starter for large-scale cloud businesses in China.

Technical cooperation with a domestic Chinese company that is a license holder

Currently MIIT seems to be more comfortable with technical cooperation models for delivery of cloud services in the PRC, in which (1) a PRC domestic capital VATS Permit holder enters into customer-facing contracts, and (2) the foreign cloud service provider enters into cooperation agreements to provide technical support to the VATS Permit-holding domestic capital company. This model is supported by the Draft Cloud Circular, which acknowledges that licensees may enter into technical cooperation arrangements provided that the PRC VATS Permit holder reports its technical cooperation to MIIT in writing. The Draft Cloud Circular has still not become law, but in

practice MIIT is implementing most of its provisions. As noted in our note of January 2017 (see our briefing <http://www.hoganlovells.com/en/publications/draft-legislation-to-affect-china-cloud-services-market-access>), the following activities are not permitted during the course of collaboration:

- a) the leasing, lending or transfer of a telecommunications services operating license to a partner in a disguised manner by any means, or providing to any partner the resources, venues, facilities or other conditions for unlawful operations;
- b) a partner entering into contracts directly with users;
- c) using only the trademark and brand of a partner to provide services to users;
- d) unlawfully providing to any partner user personal information and network data; and
- e) other activities which violate laws and regulations.

Items (b) and (c) are particularly challenging to branded overseas cloud service operators, as this means you cannot 'own the customer' and can only co-brand the cloud services.

### Cyber security law implications

On June 1, 2017, the Cyber Security Law came into effect. This is a law with

“

The cooperation relationship must be structured properly.

”

profound implications for global companies doing business in China. See our bulletin on this (<http://www.hoganlovells.com/en/publications/china-passes-controversial-cyber-security-law>). The cloud services sector is impacted in a number of important ways. Among other things, the Cyber Security Law requires:

- a) **Data localization:** Operators of “critical information infrastructure” must store personal information and “important data” collected during its operations within mainland China, unless the transfer offshore has been approved. The State Council has yet to come up with a final definition for “critical information infrastructure operator”.
- b) **Obligations to provide law enforcement assistance:** Network operators are required to maintain weblogs for six months and provide technical assistance and support to law enforcement investigations.
- c) The Security Assessment for Personal Information and Important Data Transmitted Outside of the People's Republic of China Measures (Amended) (“**Draft Rules on Overseas Data Transfers**”): issued in connection with the Cyber Security Law (see our bulletin here <http://www.hoganlovells.com/en/publications/chinas-draft-data-localisation-measures-open-for-comment>) *de facto* widen the net by imposing a variant of the

data localization measure (i.e. you cannot transfer overseas without clearing the security review) on “network operators”, which is a very broad concept that is thought to include cloud service operators in the PRC, so as to make overseas transfers of personal information and important data collected by network operators subject to a security review by the Chinese government and consent from the data subject. These rules were meant to come into effect at the same time as the Cyber Security Law, but were put on hold as they proved to be hugely controversial, especially as the scope went beyond the scope of the Cyber Security Law.

As noted above, although uncertainties exist as to scope of the Cyber Security Law and its applicability to cloud services providers and operations, it appears likely that cloud service providers with operations in mainland China will be required to:

- a) locate their service facilities and network data within mainland China, where such services are provided to customers in China; and
- b) ensure that any cross-border data transfers comply with relevant rules, including the Draft Rules on Overseas Data Transfers (when they become law).

## Analysis of shared model and conclusions

Recently announced cases involve US technology companies providing different types of cloud services, including IaaS, PaaS and SaaS on a large scale. Nevertheless, broadly speaking, they appear to have taken a similar approach to providing cloud services in China, as follows:

- a) Local VATS Permit holder(s) will enter into contracts with end customers and provide cloud services in their own name;
- b) Cloud services are co-branded;
- c) The local VATS Permit holder will operate the cloud services, while receiving technological support from its foreign partner; and
- d) Data centres to support the service offering and store the cloud service data are either owned by the local VATS Permit holder or leased from licensed third party vendors, and are located in China.

These all seem to be driven by the Draft Cloud Circular and the Cyber Security Law. However, in reality, customers are choosing to purchase these cloud services not because of the local VATS Permit holding entity that fronts the business, but the technology provided by, and the brand or co-brand of the big name behind it. Essentially, it has to be the global technology provider that will take the lead in managing the core functions of the business, so that people can get comfortable with the quality of the services provided to customers in China, many of whom are Chinese subsidiaries of their global clients. This is not easily achievable in the light of the laundry list of restrictions for such cooperations, not to mention those imposed by MIIT when the cooperation is reported to MIIT. With this in mind, the cooperation relationship must be structured properly, which means satisfying regulatory requirements while granting a minimum level of operational control that is acceptable to the global cloud services provider.

The cooperation structure may also take on board certain elements of a VIE structure. As discussed above, it is virtually impossible to adopt all the elements of a typical VIE, which will result in full control, and such attempts have in our experience been resisted by MIIT. Local partners on the other hand may be willing to accommodate a lot of onerous terms, as they are primarily incentivised by the financial benefit generated from the cloud operations. However, technical cooperations need to be reported to MIIT, which may review the terms of cooperation, so overly aggressive terms will not necessarily work.

For new-comers to the China market, no matter you are providing IaaS, PaaS or SaaS, unless you can get comfortable your model of SaaS does not require on IDC/IRC VATS Permit, you will likely need to team up with a Chinese VATS Permit holder, and structure the cooperation relationship in such a way as to strike a delicate balance between meeting regulatory requirements and achieving



operational autonomy. With our deep, practical, hands-on experience in this area, we are ideally placed to help you achieve that balance and to guide you through what can often be a tricky negotiation with your Chinese partner and/or the MIIT.

---



**Liang Xu**  
Partner, Beijing  
T +86 10 6582 9577  
liang.xu@hoganlovells.com



**Roy Zou**  
Partner, Beijing  
T +86 10 6582 9596  
roy.zou@hoganlovells.com



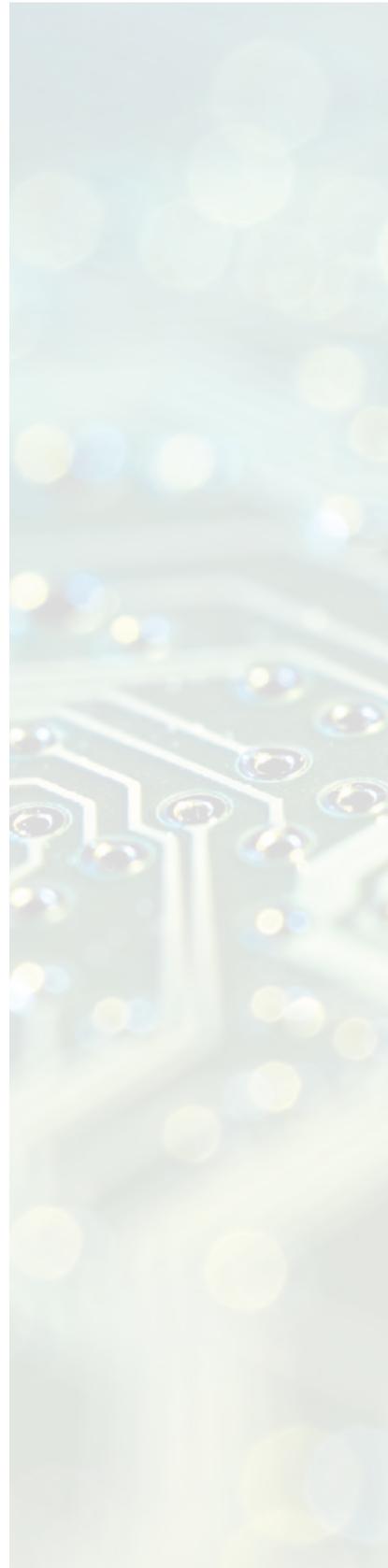
**Mo Chen**  
Associate, Beijing  
T +86 10 6582 9555  
mo.chen@hoganlovells.com



**Andrew McGinty**  
Partner, Shanghai  
T +86 21 6122 3866  
andrew.mcgintry@hoganlovells.com



**Mark Parsons**  
Partner, Hong Kong  
T +852 2840 5033  
mark.parsons@hoganlovells.com



# References

- <sup>1</sup> CBI Insights "Tracking Artificial Intelligence Hype" 5 January 2018
- <sup>2</sup> <https://deepmind.com/research/alphago/>
- <sup>3</sup> <https://www.nesta.org.uk/code-of-standards-public-sector-use-algorithmic-decision-making>
- <sup>4</sup> Google Cloud's chief scientist for AI, Fei-Fei Li, was speaking with former White House CTO Megan Smith and Foundation Capital partner Joanne Chen about the democratisation of AI at SXSWEK in Texas on 13 March 2018. For further coverage on the panel discussion, see <https://venturebeat.com/2018/03/13/google-cloud-chief-scientist-ai-doesnt-belong-to-just-a-few-tech-giants-in-silicon-valley/>.
- <sup>5</sup> Copyright, Designs and Patents Act 1988, Section 9(3)
- <sup>6</sup> Article 24(1)
- <sup>7</sup> Article 25(1).
- <sup>8</sup> Article 32.
- <sup>9</sup> <https://www.bloomberg.com/news/articles/2017-10-27/what-s-in-a-name-u-k-stock-surges-394-on-blockchain-rebrand>
- <sup>10</sup> Declaratory Ruling Report and Order, *In the Matter of Restoring Internet Freedom ("RIF Order")* WC Docket No. 17-108, p. 197 (January 4, 2018), available at [http://transition.fcc.gov/Daily\\_Releases/Daily\\_Business/2018/db0105/FCC-17-166A1.pdf](http://transition.fcc.gov/Daily_Releases/Daily_Business/2018/db0105/FCC-17-166A1.pdf).
- <sup>11</sup> *Ibid.*
- <sup>12</sup> *Ibid* at 125, 217.
- <sup>13</sup> *Ibid* at 93.
- <sup>14</sup> *Ibid* at 88, fn. 523 ("We note that FTC enforcement of Section 5 [of the FTC Act] is broader [than Section 2 of the Sherman Act] and would apply in the absence of monopoly power").
- <sup>15</sup> *Ibid.*
- <sup>16</sup> *Ibid* at 85-86.
- <sup>17</sup> *Ibid.*
- <sup>18</sup> *Ibid* at 147-154.
- <sup>19</sup> *Ibid* at 155-156.
- <sup>20</sup> *Ibid.*
- <sup>21</sup> "FCC/FTC Sign MOU to Coordinate Online Consumer Protection Efforts" (Dec. 14, 2017), available at <https://www.fcc.gov/document/fccftc-sign-mou-coordinate-online-consumer-protection-efforts>.
- <sup>22</sup> Decision, *Restoring Internet Freedom FCC-FTC Memorandum of Understanding ("MOU")* (Dec. 14, 2017), available at [https://apps.fcc.gov/edocs\\_public/attachmatch/DOC-348275A1.pdf](https://apps.fcc.gov/edocs_public/attachmatch/DOC-348275A1.pdf).
- <sup>23</sup> See *FTC v. AT&T Mobility LLC*, 835 F.3d 993 (9th Cir. 2016), reh'g en banc granted, No. 15-16585, 2017 WL 1856836 (9th Cir. May 9, 2017).
- <sup>24</sup> *RIF Order* at 113 at fn. 699.
- <sup>25</sup> Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the EU (COM(2017) 495 final)
- <sup>26</sup> Procedure 2017/0228 (COD))
- <sup>27</sup> *Schul* - Judgment of 5th May 1982 (Case 15/81)
- <sup>28</sup> Circular on Clearing-up and Standardizing the Internet Network Access Service Market, issued by MIIT on January 17, 2017.

# Notes



Alicante  
Amsterdam  
Baltimore  
Beijing  
Birmingham  
Boston  
Brussels  
Budapest  
Colorado Springs  
Denver  
Dubai  
Dusseldorf  
Frankfurt  
Hamburg  
Hanoi  
Ho Chi Minh City  
Hong Kong  
Houston  
Jakarta  
Johannesburg  
London  
Los Angeles  
Louisville  
Luxembourg  
Madrid  
Mexico City  
Miami  
Milan  
Minneapolis  
Monterrey  
Moscow  
Munich  
New York  
Northern Virginia  
Paris  
Perth  
Philadelphia  
Rio de Janeiro  
Rome  
San Francisco  
São Paulo  
Shanghai  
Shanghai FTZ  
Silicon Valley  
Singapore  
Sydney  
Tokyo  
Ulaanbaatar  
Warsaw  
Washington, D.C.  
Zagreb

Our offices

Associated offices

“Hogan Lovells” or the “firm” is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses.

The word “partner” is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members.

For more information about Hogan Lovells, the partners and their qualifications, see [www.hoganlovells.com](http://www.hoganlovells.com).

Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney advertising. Images of people may feature current or former lawyers and employees at Hogan Lovells or models not connected with the firm.

© Hogan Lovells 2018. All rights reserved. 12317\_EUn\_0518